

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-224409

(43)Date of publication of application : 21.08.1998

(51)Int.Cl.

H04L 12/66  
G06F 13/00  
G06F 13/00

(21)Application number : 09-024677

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 07.02.1997

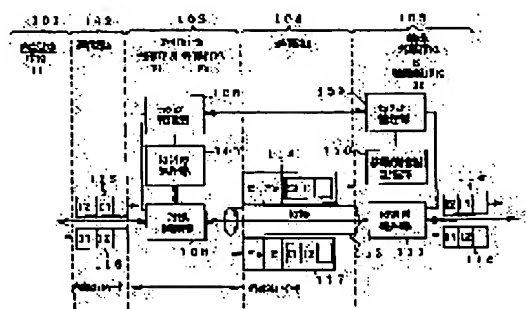
(72)Inventor : TORII TAKASHI  
NAKAGAWA SATOSHI

## (54) COMMUNICATION SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To continuously enjoy the service within a range of the application right received before a terminal set at a position in an internal network is moved to an external network by storing the terminal address that is assigned before the movement of the terminal or previously assigned in the internal network.

**SOLUTION:** When the communication is started between an internal host 101 and a terminal 105, a session management part 106 communicates with a session management part 109 to perform the authentication and key exchange to the terminal 105. The part 109 notifies the part 106 of a fact that the terminal 105 moved to an external network and an external address is equal to E and I2 after and before movement of the terminal 105 respectively. Thus, an access control part 108 relays a packet 113 between the host 101 and the terminal 105. The receiving and transmitting destination addresses of the packet 113 sent to the terminal 105 from the host 101 are equal to I2 and I1 respectively.



## LEGAL STATUS

[Date of request for examination] 15.12.2000

[Date of sending the examiner's decision of rejection] 07.12.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

NO PAGE RI ANK 05710

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-224409

(43) 公開日 平成10年(1998) 8月21日

(51) Int.Cl.<sup>6</sup>

H 0 4 L 12/66

G 0 6 F 13/00

識別記号

3 5 1

3 5 4

F I

H 0 4 L 11/20

G 0 6 F 13/00

B

3 5 1 A

3 5 4 A

審査請求 未請求 請求項の数22 O L (全 30 頁)

(21) 出願番号 特願平9-24677

(22) 出願日 平成9年(1997) 2月7日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 烏居 肖史

東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内

(72) 発明者 中川 聡

東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内

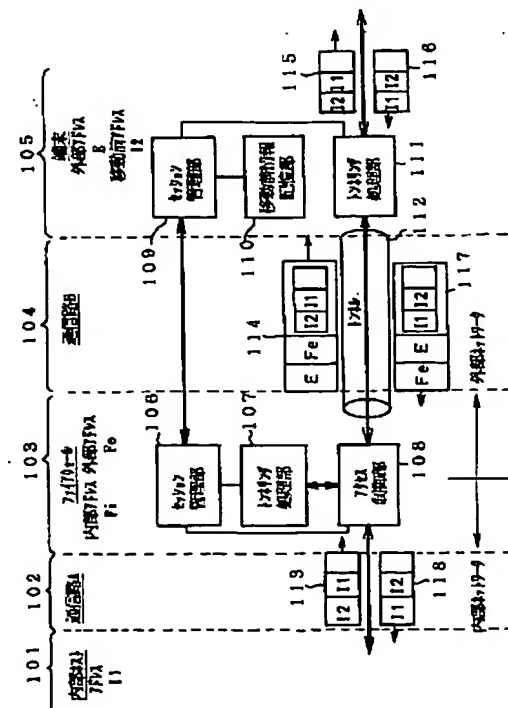
(74) 代理人 弁理士 工藤 宜幸

(54) 【発明の名称】 通信システム

(57) 【要約】

【課題】 内部ネットワークに位置する端末を外部ネットワークへ移動させると、端末のアドレスに変化が生じるため、移動前の利用権限ではサービスを受け得ない。

【解決手段】 外部ネットワークの端末に、移動前に又は予め内部ネットワークにおいて割り当てられていた端末アドレスを記憶するアドレス記憶手段を備えるようにする。これにより、外部ネットワークに位置する端末であつても内部ネットワークで割り当てられた端末アドレスを記憶する端末については、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能とできる。



**【特許請求の範囲】**

【請求項 1】 外部ネットワークに位置する端末が、ファイアウォールを介して内部ネットワークの内部ホストと通信する形態の通信システムにおいて、上記端末は、移動前に又は予め内部ネットワークにおいて割り当てられた端末アドレスを記憶するアドレス記憶手段を備えることを特徴とする通信システム。

【請求項 2】 上記端末及び上記ファイアウォールは、当該端末が内部ネットワークから外部ネットワークへ移動した場合に、上記アドレス記憶手段が記憶している端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及びファイアウォールの間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする請求項 1 に記載の通信システム。

【請求項 3】 上記端末及び上記内部ホストは、当該端末が内部ネットワークから外部ネットワークへ移動した場合に、上記アドレス記憶手段が記憶している端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及び内部ホスト間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする請求項 1 に記載の通信システム。

【請求項 4】 上記内部ネットワークにおける各サブネットのサブネット管理サーバは、上記端末が内部ネットワークから外部ネットワークへ移動した場合に、上記アドレス記憶手段が記憶している端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバと上記端末との間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする請求項 1 に記載の通信システム。

【請求項 5】 上記ファイアウォールはトンネルの内部に位置し、当該ファイアウォールは、上記パケットのヘッダのアドレスを書き換えるヘッダアドレス書換手段を備えることを特徴とする請求項 3 又は 4 に記載の通信システム。

【請求項 6】 上記ファイアウォールは、内部ネットワークに接続しているネットワーク・インターフェースのアドレスを複数有することを特徴とする請求項 5 に記載の通信システム。

【請求項 7】 上記ファイアウォールは、内部ネットワークに接続しているネットワーク・インターフェースのアドレスを複数有し、かつ、外部ネットワークに接続しているネットワーク・インターフェースのアドレスを複数有することを特徴とする請求項 5 に記載の通信システム。

【請求項 8】 上記ファイアウォールは、パケットのヘッダに記録されているセキュリティ関連情報に基づいて、上記パケットのヘッダのアドレスを書き換えることを特徴とする請求項 5 に記載の通信システム。

【請求項 9】 上記ファイアウォールは、パケットのヘ

ッダに記録されている、パケットが通過するトンネルの両端アドレスを表すフィールドの値に基づいて、上記パケットのヘッダのアドレスを書き換えることを特徴とする請求項 5 に記載の通信システム。

【請求項 10】 内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内で内部ホストと通信する形態の通信システムにおいて、

上記端末は、同じネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、上記端末及び上記内部ホストは、当該移動があった場合に、上記アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及び内部ホストの間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする通信システム。

【請求項 11】 内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、

上記端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、上記端末及び当該端末が移動前に位置したサブネットのサブネット管理サーバは、当該移動があった場合に、上記アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、上記端末及びサブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする通信システム。

【請求項 12】 内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、

上記端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、上記端末の移動の前後に係る各サブネットのサブネット管理サーバは、当該移動があった場合に、上記アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする通信システム。

【請求項 13】 上記ファイアウォールは、内部ネットワークから外部ネットワークへ移動した端末に対して外部ネットワークが割り当てた端末アドレスを記憶するアドレス記憶手段を備えることを特徴とする請求項 1～9 のいずれかに記載の通信システム。

【請求項 14】 上記内部ネットワーク内のサブネット管理サーバは、内部ネットワークから外部ネットワークへ移動した端末に対して外部ネットワークが割り当てた

端末アドレスを記憶するアドレス記憶手段を備えることを特徴とする請求項 1～9 のいずれかに記載の通信システム。

【請求項 15】 上記トンネルの両端位置に、上記パケットを暗号処理する暗号処理手段を備えることを特徴とする請求項 1～14 のいずれかに記載の通信システム。

【請求項 16】 上記トンネルの両端位置を除く内部位置に、上記パケットを暗号処理する暗号処理手段を備えることを特徴とする請求項 1～14 のいずれかに記載の通信システム。

【請求項 17】 上記暗号処理手段は、上記パケットのヘッダのアドレスに応じて、暗号処理のアルゴリズムを、1つ以上の暗号処理のアルゴリズムと恒等写像のうちのいずれかに切り替えることを特徴とする請求項 15 又は 16 に記載の通信システム。

【請求項 18】 上記暗号処理手段は、上記パケットのヘッダに記憶されているセキュリティ関連情報に応じて、暗号処理のアルゴリズムを、1つ以上の暗号処理のアルゴリズムと恒等写像のうちのどれかに切り替えることを特徴とする請求項 15 又は 16 に記載の通信システム。

【請求項 19】 上記トンネルの両端位置に、パケットを認証処理する認証処理手段を備えることを特徴とする請求項 1～14 のいずれかに記載の通信システム。

【請求項 20】 上記トンネルの両端位置を除く内部位置に、パケットを認証処理する認証処理手段を備えることを特徴とする請求項 1～14 のいずれかに記載の通信システム。

【請求項 21】 上記認証処理手段は、上記パケットのヘッダのアドレスに応じて、パケットの認証処理のアルゴリズムを変更することを特徴とする請求項 19 又は 20 に記載の通信システム。

【請求項 22】 上記認証処理手段は、上記パケットのヘッダに記憶されているセキュリティ関連情報に応じて、パケットの認証処理のアルゴリズムを変更することを特徴とする請求項 19 又は 20 に記載の通信システム。

#### 【発明の詳細な説明】

#### 【0001】

【発明の属する技術分野】 本発明は、通信システムに関し、特に、ファイアウォールを介して内外のネットワーク間で通信を行うシステムに好適なものである。

#### 【0002】

#### 【従来の技術】

文献名：R. Atkinson, "Security Architecture for the Internet Protocol", RFC1825, August 1995

従来、この種の通信システムで用いられる通信方式として、上記文献に開示されている通信方式がある。この通信方式は、外部ネットワークのホスト（外部ホスト）がファイアウォールを介して内部ネットワークのホスト

（内部ホスト）と通信する場合に、ファイアウォールが外部ホストを認証して鍵交換した後、当該ファイアウォールと外部ホストの間でパケットの暗号処理を行ってトンネリングすることで、外部ネットワークでの盗聴、改竄、なりすましを防止するものである。

【0003】ここで、トンネリングとは、WIDEプロジェクト「1994年度WIDEプロジェクト研究報告書」p137にも示されているように、ネットワーク層のプロトコル（例えばIP：Internet Protocol）を伝達するために、同じネットワーク層のプロトコル（例えばIP）をデータリンク層のプロトコルとみなして利用する技術をいう。また、トンネルとは、通信路のうちトンネリングを適用する部分をいう。

【0004】図2に、トンネル内を伝送されるパケットの構造例を示す。図2の場合、「パケットB」202が、「パケットA」201のペイロード204に格納されているが、これは、「パケットA」201が、「パケットB」202をカプセル化(encapsulation)している状態を表している。なお、あるパケットのペイロードからカプセル化されているパケットを抽出する処理を、以下、脱カプセル化(decapsulation)という。

【0005】ところで、上記文献の通信方式では、次に示す(a)～(c)の手段が必要になる。(a)の手段は、ファイアウォールが外部ホストを認証し鍵の交換を行うための手段（以下、セッション管理部という。）である。この手段は、ファイアウォールと外部ホストのそれぞれに必要とされる。(b)の手段は、ファイアウォールと外部ホストとの間でパケットを暗号処理しトンネリングするための手段（以下、トンネリング処理部という。）である。この手段も、ファイアウォールと外部ホストのそれぞれに必要とされる。(c)の手段は、アクセスを許可したパケットのみを中継しその他のパケットは遮断することにより、外部ネットワークから内部ネットワークへの不正なアクセスを防止するための手段（以下、アクセス制御部と呼ぶ。）である。この手段は、内部ネットワークと外部ネットワークの境界に設けられているファイアウォールに必要とされる。

【0006】従って、上記文献の通信方式を用いる通信システムは、図3に示す構成となる。なお、上記文献には係る構成は示されていないので、図3は、必要とされる手段を基に作成したものである。

【0007】このシステムは、内部ホスト301、「通信路A」302、ファイアウォール303、「通信路B」304、外部ホスト305からなる。このうち、「通信路A」302は、内部ホスト301とファイアウォール303間の通信路である。「通信路A」302は、内部ネットワークの通信路に当たる。一方、「通信路B」304は、ファイアウォール303と外部ホスト305間の通信路である。「通信路B」304は、外部ネットワークの通信路に当たる。ファイアウォール30

3は、前述したように(a)～(c)の3つの手段、セッション管理部306、トンネリング処理部307、アクセス制御部308からなる。また、外部ホスト305は、前述した(a)及び(b)の2つの手段、セッション管理部309、トンネリング処理部310からなる。ところで、ファイアウォール303と外部ホスト305の間にはトンネル311がある。

【0008】次に、かかる構成のシステムにおいて実行される通信動作を説明する。まず、内部ホスト301から外部ホスト305に対してパケットを送信する場合、ファイアウォール303が、パケット312を暗号処理し、さらに、図2のようにカプセル化する。カプセル化されたパケット312はパケット313として、トンネル311を伝送され外部ホスト305に達する。外部ホスト305は、これを脱カプセル化し、パケット314を得る。

【0009】この反対に、外部ホスト305から内部ホスト301にパケットを送信する場合、外部ホスト305が、パケット315を暗号処理しパケット316のようにカプセル化する。このパケット316は、トンネル311を介してファイアウォール303に達し、ここで脱パケット化されて内部ホスト301にパケット317として与えられる。

【0010】以上のようにして、双方向の通信がなされる。

#### 【0011】

【発明が解決しようとする課題】しかしながら、上記文献の通信方式の場合、内部ネットワーク上に位置する端末を、何らかの事情で外部ネットワーク上へ移動させた場合、以下に示す問題が生じてしまう。

【0012】一般に、サービスを提供するアプリケーションは、サービスを要求しているホストのアドレスに基づいて、サービスの利用権限を求める。従って、内部ネットワーク上に位置する端末を、外部ネットワーク上へ移動すると、端末のアドレスが変化するので、端末は内部ホストが提供するサービスを移動前のサービス利用権限では利用できなくなってしまう。ここで、サービス利用権限には、例えば、サービスの利用を許可すること、又は、サービスの利用を禁止すること、サービスのある品質で許可することなどがある。

【0013】本発明は以上の課題を考慮してなされたもので、内部ネットワーク上に位置していた端末を外部ネットワーク上へ移動しても、移動前に提供を受けることができたサービス利用権限の範囲内で引き続きサービスを享受できるようにするリモートアクセス通信システムを提供しようとするものである。

#### 【0014】

【課題を解決するための手段】

(A) かかる課題を解決するため第1の発明においては、外部ネットワークに位置する端末が、ファイアウォール

を介して内部ネットワークの内部ホストと通信する形態の通信システムにおいて、以下の手段を備えたことを特徴とする。

【0015】すなわち、端末は、移動前に又は予め内部ネットワークにおいて割り当てられた端末アドレスを記憶するアドレス記憶手段を備えたことを特徴とする。

【0016】このように、第1の発明における通信システムによれば、外部ネットワークに位置する端末であっても内部ネットワークで割り当てられた端末アドレスを記憶する端末については、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能となる。これにより、特定の端末については、外部ネットワークに位置する場合にも、内部ネットワークに位置する場合と同じ利用権限でのサービスを受けることができる。

【0017】(B) また、第2の発明においては、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内で内部ホストと通信する形態の通信システムにおいて、以下の手段を備えることを特徴とする。

【0018】すなわち、端末は、同じネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、端末及び内部ホストは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及び内部ホストの間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする。

【0019】このように、第2の発明における通信システムによれば、内部ネットワーク内であるサブネットから他のサブネットに端末が移動した場合にも、移動前における端末アドレスを端末が記憶しているので、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能となる。これにより、特定の端末については、他のサブネットに移動した場合にも、移動前のサブネットで許容されていたのと同じ利用権限でサービスを受けることができる。

【0020】(C) さらに、第3の発明においては、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、以下の手段を備えることを特徴とする。

【0021】すなわち、端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、端末及び当該端末が移動前に位置したサブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及びサブネット管理サーバ間

に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする。

【0022】このように、第3の発明における通信システムによれば、端末とサブネット管理サーバとの間にトンネルを設けているので、内部ホストごとに各端末までのトンネルを設けなくて良くなる。

【0023】(D) さらに、第4の発明においては、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、以下の手段を備えることを特徴とする。

【0024】すなわち、端末は、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備え、かつ、端末の移動の前後に係る各サブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えることを特徴とする。

【0025】このように、第4の発明における通信システムによれば、サブネット管理サーバ間にトンネルを設けるので、端末がトンネリング処理をせずに済み、その分、端末の負荷を軽減できるという効果が得られる。

#### 【0026】

##### 【発明の実施の形態】

##### (A) 各実施形態で用いるパケットの構造

まず、後述する各実施形態において使用されるパケットの基本構造を説明する。図4は、トンネルを介して送受されるパケットの構造を表した図である。この図4は、「パケットB」402が、「パケットA」401のペイロードに格納され、カプセル化(encapsulation)されている状態を表している。ここで、「パケットA」の受信先アドレス403と「パケットA」の送信元アドレス404が「パケットA」のヘッダを表し、「パケットB」の受信先アドレス405と「パケットB」の送信元アドレス406が「パケットB」のヘッダを表している。

【0027】ここで、「パケットB」を端末へ入力する場合は、「パケットB」の受信先アドレス405に書き込まれているアドレスが、外部ネットワーク上でのアドレスではなく、予め内部ネットワークで各端末に割り当てられた内部ネットワーク上でのアドレス(内部ネットワークから外部ネットワークへ移動する場合における移動前のアドレスを含む)が書き込まれている。各実施形態では、このアドレスを用いた通信システムについて説明する。

【0028】また、一部実施形態(第5の実施形態及び第10の実施形態)においては、図5に示す構造のパケ

ットを使用する。この図5の場合も、トンネルを介して送受されるパケットの構造を表した図であり、「パケットB」502が、「パケットA」501のペイロードに格納され、カプセル化(encapsulation)されている状態を表している。図5のパケットが図4のパケットと異なる点は、「パケットA」のヘッダが、「パケットA」の受信先アドレス503と「パケットA」の送信元アドレス504に加えて、「パケットA」のSPI(Security Parameters Index)を有する点である。ここで、SPIは、使用する暗号アルゴリズムや鍵等のセキュリティに関するパラメータを表すものである。なお、「パケットB」のヘッダの構造は同じであり、「パケットB」を端末へ入力する場合は、「パケットB」の受信先アドレス505には、予め内部ネットワークで各端末に割り当てられた内部ネットワーク上でのアドレス(内部ネットワークから外部ネットワークへ移動する場合における移動前のアドレスを含む)が書き込まれている。

##### 【0029】(B) 第1の実施形態

以下、第1の実施形態に係る通信システムを、図面を参照しながら説明する。

##### 【0030】(B-1) 第1の実施形態の構成

図1は、第1の実施形態の構成図である。この通信システムは、内部ホスト101、「通信路A」102、ファイアウォール103、「通信路B」104、端末105からなる。因みに、従来技術で説明した図3の場合には、外部ネットワーク側の受信先が外部ホスト305となっていたが、この実施形態の場合には端末105が接続されている。

【0031】ここで、「通信路A」102は、内部ホスト101とファイアウォール103の間の通信路である。「通信路A」102は、内部ネットワークの通信路である。「通信路B」104は、ファイアウォール103と端末105の間の通信路である。「通信路B」104は、外部ネットワークの通信路である。

【0032】本実施形態に係るファイアウォール103は、セッション管理部106、トンネリング処理部107、アクセス制御部108の各構成要素を有してなる。

【0033】本実施形態に係る端末105は、セッション管理部109、移動前情報記憶部110、トンネリング処理部111の各構成要素を有してなる。このうち、移動前情報記憶部110は、後述する移動前アドレス12の記憶に用いられる。

【0034】なお、ファイアウォール103と端末105の間にトンネル112を設けることにする。

【0035】内部ホスト101は、端末105のアドレスとして移動前アドレス12を使用して、パケットを「通信路A」102と送受信する。端末105は、端末105のアドレスとして移動前アドレス12を使用して、パケットをトンネリング処理部111と入出力する。

【0036】セッション管理部106とセッション管理部109は、互いに通信し、端末105の認証と鍵交換をする。セッション管理部109は、セッション管理部106へ、端末105が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であることを通知する。

【0037】トンネリング処理部107は、セッション管理部106が交換した鍵を使用して、端末105宛てのパケットを暗号処理してカプセル化する。また、トンネリング処理部107は、内部ホスト101宛てのパケットを脱カプセル化し復号処理する。

【0038】トンネリング処理部111は、セッション管理部109が交換した鍵を使用して、内部ホスト101宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部111は端末105宛てのパケットを脱カプセル化し復号処理する。

【0039】アクセス制御部108は、受信するパケットが、内部ホスト101と端末105の間の通信のパケットであるかを判定する。アクセス制御部108は、内部ホスト101と端末105の間の通信のパケットを、トンネリング処理部107へ入力してパケットを加工し、中継する。アクセス制御部108は、内部ホスト101と端末105の間の通信ではないパケットを、中継しない。

【0040】内部ホスト101のアドレスは、I1である。内部ネットワークに接続しているファイアウォール103のネットワーク・インターフェースのアドレスはFiである。外部ネットワークに接続しているファイアウォール103のネットワーク・インターフェースのアドレスはFeである。端末105のアドレスは、Eである。外部ネットワークへの移動前の端末105の内部ネットワークでのアドレス（移動前アドレス）はI2である。

【0041】（B-2）第1の実施形態の通信動作  
続いて、図1に示す通信システムによって実現される通信動作を説明する。

【0042】（B-2-1）通信開始前の動作

まず、内部ホスト101と端末105が通信を開始するまでの動作を説明する。これには、セッション管理部106とセッション管理部109とが通信し、端末105の認証と鍵交換を行う。セッション管理部109は、セッション管理部106へ、端末105が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であることを通知する。これにより、アクセス制御部108は、内部ホスト101と端末105の間のパケットを中継するようになる。

【0043】（B-2-2）通信開始後の動作

次に、内部ホスト101と端末105が通信をする時の動作を説明する。

【0044】なお、内部ホスト101から端末105へ

伝送されるパケット113の受信先アドレスはI2、送信元アドレスはI1となる。また、このパケット113をカプセル化したパケット114の受信先アドレスはE、送信元アドレスはFeとなる。これを脱パケット化した後のパケット115は、パケット113と同一となる。

【0045】一方、端末105から内部ホスト101へ伝送されるパケット116の受信先アドレスはI1、送信元アドレスはI2となる。また、このパケット116をカプセル化したパケット117の受信先アドレスはFe、送信元アドレスはEとなる。これを脱パケット化した後のパケット118は、パケット116と同一となる。

【0046】（B-2-2-1）内部ホストから端末への送信

まず、内部ホスト101から端末105にパケットを送信する場合の動作を説明する。

【0047】内部ホスト101は、「通信路A」102に対してパケット113を送信する。

【0048】ファイアウォール103のアクセス制御部108は、「通信路A」102からパケット113を受信する。アクセス制御部108は、そのヘッダから、パケット113は内部ホスト101と端末105間のパケットであると判定する。アクセス制御部108は、パケット113をトンネリング処理部107へ与える。トンネリング処理部107は、セッション管理部106が交換した鍵を使用して、パケット113を暗号処理してカプセル化し、パケット114を得る。この時、パケット113の受信先アドレスがI2であるので、パケット114の受信先アドレスをEとする。かかる後、トンネリング処理部107は、パケット114をアクセス制御部108に与える。アクセス制御部108は、このパケット114を「通信路B」104へ送信する。

【0049】端末105のトンネリング処理部111は、「通信路B」104からパケット114を受信する。トンネリング処理部111は、セッション管理部109が交換した鍵を使用して、パケット114を脱カプセル化し復号処理し、パケット115を得る。端末105は、トンネリング処理部111からパケット115を得る。

【0050】（B-2-2-2）端末から内部ホストへの送信

逆に、端末105から内部ホスト101にパケットを送信する場合の動作を説明する。

【0051】端末105は、パケット116をトンネリング処理部111へ入力する。トンネリング処理部111は、セッション管理部109が交換した鍵を使用して、パケット116を暗号処理してカプセル化し、パケット117を得る。トンネリング処理部111は、「通信路B」104へパケット117を送信する。



【0052】ファイアウォール103のアクセス制御部108は、「通信路B」104からパケット117を受信する。アクセス制御部108は、パケット117は内部ホスト101と端末105の間のパケットであると判定する。アクセス制御部108は、パケット117をトンネリング処理部107へ入力する。トンネリング処理部107は、セッション管理部106が交換した鍵を使用して、パケット117を脱カプセル化し復号処理し、パケット118を得る。トンネリング処理部107は、パケット118をアクセス制御部108へ出力する。アクセス制御部108は、「通信路A」102へパケット118を送信する。

【0053】内部ホスト101は、パケット118を受信する。

【0054】(B-2-3) 通信終了動作  
内部ホスト101と端末105が通信を終了する場合の動作を説明する。

【0055】ファイアウォール103が通信の終了を要求する場合には、セッション管理部106がセッション管理部109に通信の終了を要求する。これに対して、端末105が通信の終了を要求する場合には、セッション管理部109がセッション管理部106に通信の終了を要求する。

【0056】ファイアウォール103が「通信路B」104から受信するパケットには、アクセス制御部106が受信するパケットとセッション管理部106が受信するパケットがある。ファイアウォール103は、パケットのヘッダのうちアドレス以外の値により、どちらのパケットであるかを判定する。端末105が「通信路B」104から受信するパケットについても同様である。

【0057】(B-2-4) 内部ネットワークに対するサービスの提供

ファイアウォール103が内部ネットワーク向けにサービスを提供している場合について説明する。

【0058】この場合は、アクセス制御部108は、「通信路A」102と送受信するパケット(パケット113とパケット118)を、ファイアウォール103と入出力する。

【0059】(B-3) 第1の実施形態の効果  
以上のように、第1の実施形態によれば、ファイアウォールと外部の端末との間にトンネルを設け、そのトンネルにおいて、端末アドレスに移動前アドレスを使用するパケットをカプセル化するようにしたので、内部ネットワークに位置する端末を外部ネットワークへ移動しても、内部ホストに対しては、端末のアドレスが外部ネットワークへの移動前後で変化していないようにみなせるので、端末は内部ホストが提供するサービスを移動前のサービス利用権限で利用できるといった効果が得られる。

【0060】また、これらサービスは、パケット伝送により実現されるので、複数の内部ホスト101と複数の

端末105間において同時通信を実現できる。

【0061】(C) 第2の実施形態

続いて、第2の実施形態を説明する。ところで、前述の第1の実施形態が有効に機能するには、内部ネットワークにおいて、受信先アドレスが端末の移動前アドレスI2であるパケットがファイアウォールに届かなければならず、届かない場合には外部ネットワークに移動した端末との間で通信できない。例えば、内部ホストと移動前の端末との間の経路にファイアウォールが位置しない場合には、ルータの経路制御テーブルを変更しないと、受信先アドレスが端末の移動前アドレスI2であるパケットをファイアウォールに届けることができない。そこで、次の実施形態を考える。

【0062】(C-1) 第2の実施形態の構成

図6は、第2の実施形態の構成図である。この通信システムは、内部ホスト601、「通信路A」602、ファイアウォール603、「通信路B」604、端末605からなる。ここで、「通信路A」602は、内部ホスト601とファイアウォール603の間の通信路であり、内部ネットワークの通信路である。「通信路B」604は、ファイアウォール603と端末605の間の通信路である。「通信路B」604は、外部ネットワークの通信路である。

【0063】この実施形態では、第1の実施形態においてはファイアウォールに設けられていた3つの構成要素のうち2つの構成要素が内部ホスト601側に設けるようにしている。すなわち、本実施形態に係る内部ホスト601は、セッション管理部606、トンネリング処理部607を構成要素にもつ。

【0064】一方、本実施形態に係るファイアウォール603の構成要素は、セッション管理部608、アクセス制御部609の2つである。

【0065】本実施形態に係る端末605の構成要素は、第1の実施形態の場合と同じ、すなわち、セッション管理部610、移動前情報記憶部611、トンネリング処理部612の3つである。ここで、移動前情報記憶部611は、端末605の移動前アドレスI2、内部ホスト601のアドレスI1を記憶している。

【0066】なお、本実施形態の場合には、2つのトンネルを用意する。1つは、内部ホスト601とファイアウォール603の間のトンネル613であり、1つは、ファイアウォール603と端末605の間のトンネル614である。

【0067】内部ホスト601は、端末605のアドレスとして移動前アドレスI2を使用して、パケットをトンネリング処理部607と入出力する。

【0068】端末605は、端末605のアドレスとして移動前アドレスI2を使用して、パケットをトンネリング処理部612と入出力する。

【0069】セッション管理部608とセッション管理

部 610 は、互いに通信し、端末 605 の認証と鍵交換をする。ここで、セッション管理部 610 は、セッション管理部 608 へ、端末 605 が外部ネットワークへ移動したこと、移動後のアドレスが E であること、移動前アドレスが I2 であること、内部ホスト 601 のアドレスが I1 であることを通知する。一方、セッション管理部 608 は、セッション管理部 606 へ、端末 605 が外部ネットワークへ移動したこと、移動後のアドレスが E であること、移動前アドレスが I2 であること、及び鍵を通知する。

【0070】トンネリング処理部 607 は、セッション管理部 608 が交換した鍵を使用して、端末 605 宛ての packets を暗号処理しカプセル化する。また、トンネリング処理部 607 は、内部ホスト 601 宛ての packets を脱カプセル化し復号処理する。

【0071】トンネリング処理部 612 は、セッション管理部 610 が交換した鍵を使用して、内部ホスト 601 宛ての packets を暗号処理しカプセル化する。また、トンネリング処理部 612 は、端末 605 宛ての packets を脱カプセル化し復号処理する。

【0072】アクセス制御部 609 は、受信する packets が、内部ホスト 601 と端末 605 の間の通信の packets であるかを判定する。アクセス制御部 609 は、内部ホスト 601 と端末 605 の間の通信の packets を中継する。アクセス制御部 609 は、内部ホスト 601 と端末 605 の間の通信ではない packets を中継しない。

【0073】(C-2) 第 2 の実施形態の動作  
続いて、図 6 に示す通信システムによって実現される通信動作を説明する。

【0074】(C-2-1) 通信開始前の動作

まず、内部ホスト 601 と端末 605 が通信を開始するまでの動作を説明する。

【0075】セッション管理部 608 とセッション管理部 610 が通信し、端末 605 の認証と鍵交換をする。セッション管理部 610 は、セッション管理部 608 へ、端末 605 が外部ネットワークへ移動したこと、移動後のアドレスが E であること、移動前アドレスが I2 であること、内部ホスト 601 のアドレスが I1 であることを通知する。セッション管理部 608 は、セッション管理部 606 へ、端末 605 が外部ネットワークへ移動したこと、移動後のアドレスが E であること、移動前アドレスが I2 であること、及び鍵を通知する。これにより、アクセス制御部 609 は、内部ホスト 601 と端末 605 の間の packets を中継するようになる。

【0076】(C-2-2) 通信開始後の動作  
次に、内部ホスト 601 と端末 605 が通信する時の動作を説明する。

【0077】なお、内部ホスト 601 から端末 605 へ伝送される packets 615 の受信先アドレスは I2、送信元アドレスは I1 となる。また、この packets 615

をカプセル化した packets 616 の受信先アドレスは E、送信元アドレスは I1 となる。なお、packets 617 は、packets 616 と同一である。packets 618 は、packets 615 と同一である。

【0078】一方、端末 605 から内部ホスト 601 へ伝送される packets 619 の受信先アドレスは I1、送信元アドレスは I2 となる。また、この packets 619 をカプセル化した packets 620 の受信先アドレスは I1、送信元アドレスは E となる。なお、packets 621 は、packets 620 と同一である。packets 622 は、packets 619 と同一である。

【0079】(C-2-2-1) 内部ホストから端末への送信

まず、内部ホスト 601 から端末 605 に packets を送信する場合の動作を説明する。

【0080】内部ホスト 601 は、packets 615 をトンネリング処理部 607 へ入力する。トンネリング処理部 607 は、セッション管理部 608 が交換した鍵を使用して、packets 615 を暗号処理しカプセル化し packets 616 を得る。この時、packets 615 の受信先アドレスが I2 であるので、packets 616 の受信先アドレスを E にする。トンネリング処理部 607 は、「通信路 A」602 へ packets 616 を送信する。

【0081】ファイアウォール 603 のアクセス制御部 609 は、「通信路 A」602 から packets 616 を受信する。アクセス制御部 609 は、packets 616 が内部ホスト 601 と端末 605 の間の packets であると判定する。アクセス制御部 609 は、「通信路 B」604 へ packets 617 を送信する。トンネリング処理部 612 は、「通信路 B」604 から packets 617 を受信する。トンネリング処理部 612 は、セッション管理部 610 が交換した鍵を使用して、packets 617 を脱カプセル化し復号処理し、packets 618 を得る。

【0082】端末 605 は、トンネリング処理部 612 から packets 618 を得る。

【0083】(C-2-2-2) 端末から内部ホストへの送信

逆に、端末 605 から内部ホスト 601 に packets を送信する場合の動作を説明する。

【0084】端末 605 は、packets 619 をトンネリング処理部 612 へ入力する。トンネリング処理部 612 は、セッション管理部 610 が交換した鍵を使用して、packets 619 を暗号処理しカプセル化し packets 620 を得る。この時、packets 619 の受信先アドレスが I1 であるので、packets 620 の受信先アドレスを I1 にする。

【0085】ファイアウォール 603 のアクセス制御部 609 は、packets 620 が内部ホスト 601 と端末 605 の間の packets であると判定し、packets 620 を中継する。

【0086】内部ホスト601のトンネリング処理部607は、セッション管理部608が交換した鍵を使用して、パケット621を脱カプセル化し復号処理しパケット622を得る。

【0087】(C-3)第2の実施形態の効果

以上のように、第2の実施形態によれば、内部ホストと端末との間にトンネルを設けるので、内部ネットワークにおいて、受信先アドレスが端末の移動前アドレス12であるパケットがファイアウォールに届かない場合であっても、ルーティングテーブルを変更することなく経路制御をすることができる。これにより、外部ネットワークに移動した端末は任意の内部ホストにアクセスできるようになる。

【0088】また、第2の実施形態によれば、複数の内部ホスト601と複数の端末605が同時に通信可能である。

【0089】(D)第3の実施形態

続いて、第3の実施形態を説明する。ところで、第2の実施形態では、外部ネットワークにおいて、ヘッダに内部ホストのアドレスを含むパケットを伝送する形態となるため、外部ネットワークにおいて内部ホストのアドレスを隠蔽できない。そこで、次の実施形態を考える。

【0090】(D-1)第3の実施形態の構成

図7は、第3の実施形態の構成図である。この通信システムの場合も基本構成は、内部ホスト701、「通信路A」702、ファイアウォール703、「通信路B」704、端末705である。なお、図7は、図6との対応部分に対応符号を付して示すもので、セッション管理部706～トンネリング処理部712は、それぞれ、図6のセッション管理部606～トンネリング処理部612に対応している。これらの構成は、第2の実施形態の場合と同様である。また、トンネル内のパケットを除く各パケット715、718、719、722も、第2の実施形態の場合と同様である。

【0091】従って、本実施形態と第2の実施形態との違いは、本実施形態に係るファイアウォール703がアドレス変換部723を構成要素として有している点にある。このアドレス変換部723は、ファイアウォール703のアクセス制御部709が中継するパケットのヘッダアドレスを書き換える役割をもつものである。

【0092】(D-2)第3の実施形態の動作

続いて、図7に示す通信システムによって実現される通信動作を説明する。なお、以下の説明では、第3の実施形態の動作のうち、第2の実施形態の動作と異なる動作を重点的に説明することにする。

【0093】(D-2-1)通信開始前の動作

まず、内部ホスト701と端末705が通信を開始するまでの動作であるが、これは、第2の実施形態の場合と同様である。すなわち、セッション管理部706と708及びセッション管理部708と710の間で通信がな

され、端末705の移動が通知される。

【0094】(D-2-2)通信開始後の動作

次に、内部ホスト701と端末705が通信する時の動作を説明する。

【0095】ただし、この実施形態の場合には、内部ホスト701から端末705へ伝送されるパケット715をカプセル化したパケット716の受信先アドレスがFi、送信元アドレスがI1となる。しかも、このパケット716のアドレスは書き換えの対象となるので、パケット717の受信先アドレスはE、送信元アドレスはFeとなる。その反対に、端末705から内部ホスト701へ伝送されるパケット719をカプセル化したパケット720の受信先アドレスはFe、送信元アドレスはEとなる。また同様に、パケット721の受信先アドレスはI1、送信元アドレスはFiとなる。

【0096】(D-2-2-1)内部ホストから端末への送信

まず、内部ホスト701から端末705にパケットを送信する場合の動作を説明する。

【0097】アクセス制御部709がパケット716は内部ホスト701と端末705の間の通信のパケットであると判定するまでの動作は、第2の実施形態の場合と同様である。

【0098】アクセス制御部709は、パケット716をアドレス変換部723に入力する。アドレス変換部723は、パケット716のヘッダのアドレスを書き換え、パケット717を得る。この時、パケット716の送信元アドレスがI1であるので、パケット717の受信先アドレスをEにする。アドレス変換部723は、アクセス制御部709へパケット717を出力する。

【0099】端末705がパケット718を得るまでの動作は、第2の実施形態と同様である。

【0100】(D-2-2-2)端末から内部ホストへの送信

逆に、端末705から内部ホスト701にパケットを送信する場合の動作を説明する。

【0101】アクセス制御部709がパケット720が内部ホスト701と端末705の間の通信のパケットであると判定するまでの動作は、第2の実施形態と同様である。

【0102】アクセス制御部709は、パケット720をアドレス変換部723に入力する。アドレス変換部723は、パケット720のヘッダのアドレスを書き換え、パケット721を得る。この時、パケット720の送信元アドレスがEであるので、パケット721の受信先アドレスをI1にする。

【0103】アドレス変換部723は、アクセス制御部709にパケット721を出力する。内部ホスト701がパケット722を得るまでの動作は、第2の実施形態と同様である。

【0104】(D-3) 第3の実施形態の効果  
 以上のように、第3の実施形態によれば、ファイアウォールにアドレスを変換する機能を備えたので、外部ネットワークに、内部ホストのアドレスを隠蔽できるという効果が得られる。

【0105】(E) 第4の実施形態  
 続いて、第4の実施形態を説明する。ところで、第3の実施形態では、内部ホスト701から端末705へパケットを送信する場合に、パケット716の送信元アドレス11により、パケット717の受信先アドレスEを決定する。また、端末705から内部ホスト701へパケットを送信する場合に、パケット720の送信元アドレスEにより、パケット721の受信先アドレスI1を決定する。従って、外部ネットワークに移動した端末705が、ある内部ホスト701と通信中の場合には、外部ネットワークに移動した他の端末705は、同じ内部ホスト701と同時に通信を行うことができない。そこで、次の構成を考える。

【0106】(E-1) 第4の実施形態の構成  
 図8は、第4の実施形態の構成図である。この通信システムの場合も基本構成は、内部ホスト801、「通信路A」802、ファイアウォール803、「通信路B」804、端末805である。また、図7との対応部分に対応符号を付して示した図8から分かるように、これらを構成する各構成要素も基本的には、第3の実施形態と同じである。

【0107】本実施形態が第3の実施形態と異なっているのは、ファイアウォール803が、外部ネットワークに接続しているネットワーク・インターフェースのアドレスと内部ネットワークに接続しているネットワーク・インターフェースのアドレスをそれぞれ複数有する点である。すなわち、ファイアウォール803は、外部ネットワークに接続しているネットワーク・インターフェースのアドレスとしてF e 1 ~ F e n (n > 1) を有し、内部ネットワークに接続しているネットワーク・インターフェースのアドレスとしてF i 1 ~ F i m (m > 1) を有する点である。

【0108】この点について生じる違いを説明する。セッション管理部808とセッション管理部810は、互いに通信し、端末805の認証と鍵交換をする。ここで、セッション管理部810は、セッション管理部808へ、端末805が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、内部ホスト801のアドレスがI1であることを通知する。

【0109】セッション管理部808は、複数のアドレスF e 1 ~ F e n のうち、その時点で使用していないアドレスF e i を求める。セッション管理部808は、F i 1 ~ F i m のうち、その時点で使用していないアドレスF i j を求める。セッション管理部808は、セッシ

ョン管理部810に、内部ホスト801と端末805の通信で使用するファイアウォール803の外部アドレスがF e i であることを通知する。

【0110】セッション管理部808は、セッション管理部806へ、端末805が外部ネットワークへ移動したこと、移動前アドレスがI2であること、内部ホスト801と端末805の通信で使用するファイアウォール803の内部アドレスがF i j であることを、鍵を通知する。

10 【0111】(E-2) 第4の実施形態の動作  
 続いて、図8に示す通信システムによって実現される通信動作を説明する。なお、以下の説明では、第4の実施形態の動作のうち、第3の実施形態の動作と異なる動作を重点的に説明することにする。

【0112】(E-2-1) 通信開始前の動作  
 まず、内部ホスト801と端末805が通信を開始するまでの動作を説明する。

20 【0113】セッション管理部808とセッション管理部810は、互いに通信し、端末805の認証と鍵交換をする。セッション管理部810は、セッション管理部808へ、端末805が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、内部ホスト801のアドレスがI1であることを通知する。

【0114】セッション管理部808は、複数有するF e 1 ~ F e n のうち、その時点で使用していないアドレスF e i を求める。セッション管理部808は、F i 1 ~ F i m のうち、その時点で使用していないアドレスF i j を求める。

30 【0115】セッション管理部808は、セッション管理部810へ、内部ホスト801と端末805の通信で使用するファイアウォール803の外部アドレスがF e i であることを通知する。また、セッション管理部808は、セッション管理部806へ、端末805が外部ネットワークへ移動したこと、移動前アドレスがI2であること、内部ホスト801と端末805の通信で使用するファイアウォール803の内部アドレスがF i j であることを、鍵を通知する。

40 【0116】(E-2-2) 通信開始後の動作  
 次に、内部ホスト801と端末805が通信する場合の動作を説明する。なおここでは、第4の実施形態の動作のうち、第2の実施形態の動作とは異なる動作を説明する。

【0117】なお、内部ホスト801から端末805へ伝送されるパケット815の受信先アドレスはI2、送信元アドレスはI1となる。また、このパケット815をカプセル化したパケット816の受信先アドレスはF i j、送信元アドレスはI1となる。なお、パケット817は、パケット816のヘッダのアドレスを書き換えたパケットであり、その受信先アドレスはE、送信元ア

ドレスは F e i である。パケット 8 1 8 は、パケット 8 1 5 と同一である。

【0 1 1 8】一方、端末 8 0 5 から内部ホスト 8 0 1 へ伝送されるパケット 8 1 9 の受信先アドレスは I 1、送信元アドレスは I 2 となる。また、このパケット 8 1 9 をカプセル化したパケット 8 2 0 の受信先アドレスは F e i、送信元アドレスは E となる。パケット 8 2 1 は、パケット 8 2 0 のヘッダのアドレスを書き換えたパケットであり、その受信先アドレスは I 1、送信元アドレスは F i j となる。パケット 8 2 2 は、パケット 8 1 9 と同一である。

【0 1 1 9】(E-2-2-1) 内部ホストから端末への送信

まず、内部ホスト 8 0 1 から端末 8 0 5 にパケットを送信する場合の動作を説明する。

【0 1 2 0】トンネリング処理部 8 0 7 は、パケット 8 1 5 の受信先アドレスが I 2 であるので、パケット 8 1 6 の受信先アドレスを F i j にする。

【0 1 2 1】ファイアウォール 8 0 3 のアドレス変換部 8 2 3 は、パケット 8 1 6 の受信先アドレスが F i j であるので、パケット 8 1 7 の受信先アドレスを E にする。

【0 1 2 2】(E-2-2-2) 端末から内部ホストへの送信

逆に、端末 8 0 5 から内部ホスト 8 0 1 にパケットを送信する場合の動作を説明する。

【0 1 2 3】トンネリング処理部 8 1 2 は、パケット 8 1 9 の受信先アドレスが I 1 であるので、パケット 8 2 0 の受信先アドレスを F e i にする。

【0 1 2 4】ファイアウォール 8 0 3 のアドレス変換部 8 2 3 は、パケット 8 2 0 の受信先アドレスが F e i であるので、パケット 8 2 1 の受信先アドレスを I 1 にする。

【0 1 2 5】(E-3) 第 4 の実施形態の効果

以上のように、第 4 の実施形態によれば、ファイアウォールの外部アドレスと内部アドレスを複数にしたので、複数の内部ホストと複数の端末が同時に通信可能となる効果が得られる。

【0 1 2 6】(F) 第 5 の実施形態

続いて、第 5 の実施形態を説明する。ところで、第 4 の実施形態では、ファイアウォールに複数の外部アドレスと複数の内部アドレスを割り当てる必要がある。そこで、次の構成を考える。

【0 1 2 7】(F-1) 第 5 の実施形態の構成

従来技術に示した文献においては、カプセル化した後のパケットのヘッダには、受信先アドレスと送信元アドレス以外に、S P I (Security Parameters Index) を含む。S P I により、使用する暗号アルゴリズムや鍵などのセキュリティに関係するパラメータを表している。パケットを受信するコンピュータは、S P I を決めて、パ

ケットを送信するコンピュータに、S P I を通知する。

【0 1 2 8】そこで、第 5 の実施形態においては、パケットがどの内部ホストとどの端末の間の通信のパケットであるかを、S P I により表すことにする。

【0 1 2 9】図 9 は、第 5 の実施形態の構成図である。図 9 は、第 3 の実施形態の説明に用いた図 7 との対応部分に対応符号を付したものである。従って、ここでは、本実施形態の構成のうち、第 3 の実施形態の構成と異なる部分を説明する。

10 【0 1 3 0】セッション管理部 9 0 8 とセッション管理部 9 1 0 は、互いに通信し、端末 9 0 5 の認証と鍵交換をする。

【0 1 3 1】セッション管理部 9 1 0 は、内部ホスト 9 0 1 が端末 9 0 5 へ送信するパケットの S P I (ここでは B とする。)を求める。セッション管理部 9 1 0 は、セッション管理部 9 0 8 へ、端末 9 0 5 が外部ネットワークへ移動したこと、移動後のアドレスが E であること、移動前アドレスが I 2 であること、内部ホスト 9 0 1 のアドレスが I 1 であること、内部ホスト 9 0 1 が端末 9 0 5 へ送信するパケットの S P I が B であることを通知する。

【0 1 3 2】セッション管理部 9 0 8 は、セッション管理部 9 0 6 へ、端末 9 0 5 が外部ネットワークへ移動したこと、移動後のアドレスが E であること、移動前アドレスが I 2 であること、内部ホスト 9 0 1 が端末 9 0 5 へ送信するパケットの S P I が B であること、鍵を通知する。

【0 1 3 3】セッション管理部 9 0 6 は、端末 9 0 5 が内部ホスト 9 0 1 へ送信するパケットの S P I (ここでは、A とする。)を求める。セッション管理部 9 0 6 は、セッション管理部 9 0 8 へ、端末 9 0 5 が内部ホスト 9 0 1 へ送信するパケットの S P I が A であることを通知する。セッション管理部 9 0 8 は、セッション管理部 9 1 0 へ、端末 9 0 5 が内部ホスト 9 0 1 へ送信するパケットの S P I が A であることを通知する。

【0 1 3 4】トンネリング処理部 9 0 7 は、パケット 9 1 5 をカプセル化する時に、S P I を B にする。トンネリング処理部 9 1 2 は、パケット 9 1 9 をカプセル化する時に、S P I を A にする。

40 【0 1 3 5】アドレス変換部 9 2 3 は、S P I により、パケットのヘッダのアドレスを書き換える。

【0 1 3 6】(F-2) 第 5 の実施形態の動作

続いて、図 9 に示す通信システムによって実現される通信動作を説明する。

【0 1 3 7】(F-2-1) 通信開始前の動作

まず、内部ホスト 9 0 1 と端末 9 0 5 が通信を開始するまでの動作を説明する。

【0 1 3 8】セッション管理部 9 0 8 とセッション管理部 9 1 0 は、互いに通信し、端末 9 0 5 の認証と鍵交換をする。

【0139】セッション管理部910は、内部ホスト901が端末905へ送信するパケットのSPI（ここではBとする。）を求める。セッション管理部910は、セッション管理部908へ、端末905が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、内部ホスト901のアドレスがI1であること、内部ホスト901が端末905へ送信するパケットのSPIがBであることを通知する。

【0140】セッション管理部908は、セッション管理部906へ、端末905が外部ネットワークへ移動したこと、移動前アドレスがI2であること、内部ホスト901が端末905へ送信するパケットのSPIがBであること、鍵を通知する。

【0141】セッション管理部906は、端末905が内部ホスト901へ送信するパケットのSPI（ここでは、Aとする。）を求める。セッション管理部906は、セッション管理部908へ、端末905が内部ホスト901へ送信するパケットのSPIがAであることを通知する。

【0142】セッション管理部908は、セッション管理部910へ、端末905が内部ホスト901へ送信するパケットのSPIがAであることを通知する。

【0143】（F-2-2）通信開始後の動作  
次に、内部ホスト901と端末905が送信する場合の動作を説明する。なおここでは、第5の実施形態の動作のうち、第3の実施形態の動作とは異なる動作を説明する。

【0144】なお、内部ホスト901から端末905へ伝送されるパケット915の受信先アドレスはI2、送信元アドレスはI1となる。また、このパケット915をカプセル化したパケット916の受信先アドレスはFi、送信元アドレスはI1、SPIはBである。パケット917は、パケット916のヘッダのアドレスを書き換えたパケットであり、受信先アドレスはE、送信元アドレスはFe、SPIはBである。パケット918は、パケット915と同一である。

【0145】一方、端末905から内部ホスト901へ伝送されるパケット919の受信先アドレスはI1、送信元アドレスはI2となる。パケット920は、このパケット919をカプセル化したパケットであり、その受信先アドレスはFe、送信元アドレスはE、SPIはAとなる。パケット921は、パケット920のヘッダのアドレスを書き換えたパケットであり、受信先アドレスはI1、送信元アドレスはFi、SPIはAである。パケット922は、パケット919と同一である。

【0146】（F-2-2-1）内部ホストから端末への送信  
内部ホスト901から端末905にパケットを送信する場合の動作を説明する。

【0147】内部ホスト901は、パケット915をトンネリング処理部907に入力する。トンネリング処理部907は、パケット915を暗号処理しカプセル化しパケット916を得る。この時、パケット915の受信先アドレスがI2であるので、パケット916のSPIをBとする。トンネリング処理部907はパケット916を「通信路A」902に送信する。

【0148】ファイアウォール903のアクセス制御部909は、「通信路A」902からパケット916を受信する。アクセス制御部909は、パケット916をアドレス変換部923に入力する。アドレス変換部923は、パケット916のヘッダのアドレスを書き換え、パケット917を得る。この時、パケット916のSPIがBであることから、パケット917の受信先アドレスをEとする。

【0149】端末905がパケット918を得るまでの動作は、第3の実施形態と同様である。

【0150】（F-2-2-2）端末から内部ホストへの送信

逆に、端末905から内部ホスト901にパケットを送信する場合の動作を説明する。

【0151】端末905は、パケット919をトンネリング処理部912へ入力する。トンネリング処理部912は、パケット919を暗号処理しカプセル化しパケット920を得る。この時、パケット919の受信先アドレスがI1であるので、パケット920のSPIをAとする。トンネリング処理部912は、「通信路B」904にパケット920を送信する。

【0152】ファイアウォール903のアクセス制御部909は、「通信路B」904からパケット920を受信する。アクセス制御部909は、パケット920をアドレス変換部923に入力する。アドレス変換部923は、パケット920のヘッダのアドレスを書き換えパケット921を得る。この時、パケット920のSPIがAであることから、パケット921の受信先アドレスをI1とする。

【0153】内部ホスト901がパケット922を得るまでの動作は、実施形態3の動作と同様である。

【0154】（F-3）第5の実施形態の効果

以上のように、第5の実施形態によれば、パケットヘッダに書き込まれているSPIにより、パケットがどの内部ホストとどの端末の間の通信のパケットであるかを表すようにしたので、ファイアウォールに複数の外部アドレスと複数の内部アドレスを割り当てなくても、複数の内部ホストと複数の端末が同時に通信可能となる効果が得られる。

【0155】（G）第6の実施形態

続いて、第6の実施形態を説明する。ところで、第2、第3、第4、第5の実施形態では、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの

他のサブネットへ移動すると、端末のアドレスが変化するので、端末は移動前のサービス利用権限で内部ホストが提供するサービスを利用できなくなることがある。そこで、次の構成を考える。

【0156】なお、第6の実施形態では、端末が外部ネットワークに移動する場合に係る構成と動作は、第2の実施形態と同様である。以下では、第6の実施形態の構成と動作のうち、第2の実施形態の構成と動作とは異なる構成と動作を説明する。

【0157】(G-1)第6の実施形態の構成

図10は、第6の実施形態の構成図である。図10には、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネット(サブネットA)へ移動する場合に係る構成要素のみを示してある。また、図10は、端末を外部ネットワークへ移動する場合に係る構成要素の一部を示したものである。従って、図10では、内部ホスト1001、「通信路C」1002、端末1003の3つのみを示している。

【0158】本実施形態に係る内部ホスト1001は、外部セッション管理部1004、内部セッション管理部1005、トンネリング処理部1006を構成要素としてもつ。

【0159】本実施形態に係る端末1003は、内部セッション管理部1007、外部セッション管理部1008、移動前情報記憶部1009、トンネリング処理部1010を構成要素としてもつ。

【0160】また、内部ホスト1001と端末1003の間にトンネル1011を設ける。

【0161】ここで、「通信路C」1002は、内部ホスト1001と端末1003の間の通信路である。すなわち、「通信路C」1002は、内部ネットワークの通信路である。

【0162】また、第2の実施形態と同様、ファイアウォールの構成要素は、セッション管理部とアクセス制御部である。内部ホスト1001とファイアウォールとの間には、「通信路A」とトンネルがある。ファイアウォールと外部ネットワークに移動した端末との間には、「通信路B」とトンネルがある。

【0163】外部セッション管理部1008とファイアウォールのセッション管理部は、互いに通信し、外部ネットワークに移動した端末の認証と鍵交換をする。外部セッション管理部1008は、ファイアウォールのセッション管理部へ、端末が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、内部ホスト1001のアドレスがI1であることを、通知する。

【0164】ファイアウォールのセッション管理部は、外部セッション管理部1004へ、端末が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、鍵を通知する。

【0165】内部セッション管理部1005と内部セッション管理部1007は、互いに通信し、端末1003の認証と鍵交換をする。内部セッション管理部1007は、内部セッション管理部1005へ、端末1003が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがI2'であること、移動前アドレスがI2であることを通知する。

【0166】トンネリング処理部1006は、内部セッション管理部1005が交換した鍵を使用して、端末1003宛ての packets を暗号処理してカプセル化する。

【0167】また、トンネリング処理部1006は、外部セッション管理部1004が交換した鍵を使用して、外部ネットワークへ移動した端末宛ての packets を暗号処理してカプセル化する。トンネリング処理部1006は、内部ホスト1001宛ての packets を脱カプセル化し復号処理する。

【0168】トンネリング処理部1010は、内部セッション管理部1007が交換した鍵を使用して、内部ホスト1001宛ての packets を暗号処理しカプセル化する。また、トンネリング処理部1010は、外部セッション管理部1008が交換した鍵を使用して、内部ホスト1001宛ての packets を暗号処理しカプセル化する。トンネリング処理部1010は、端末1003宛ての packets を脱カプセル化し復号処理する。

【0169】(G-2)第6の実施形態の動作  
続いて、図10に示す通信システムによって実現される通信動作を説明する。

【0170】(G-2-1)通信開始前の動作

まず、内部ホスト1001と端末1003の通信の開始における動作を説明する。

【0171】内部セッション管理部1005と内部セッション管理部1007は、互いに通信し、端末1003の認証と鍵交換をする。

【0172】内部セッション管理部1007は、内部セッション管理部1005に、端末1003が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがI2'であること、移動前アドレスがI2であることを通知する。

【0173】(G-2-2)通信開始後の動作

次に、内部ホスト1001と端末1003が通信をする時の動作を説明する。

【0174】なお、内部ホスト1001から端末1003へ伝送される packets 1012の受信先アドレスはI2、送信元アドレスはI1となる。また、この packets 1012をカプセル化した packets 1013の受信先アドレスはI2'、送信元アドレスはI1である。 packets 1014は、 packets 1012と同一である。

【0175】一方、端末1003から内部ホスト1001へ伝送される packets 1015の受信先アドレスはI1、送信元アドレスはI2となる。 packets 1016



は、このパケット1015をカプセル化したパケットであり、その受信先アドレスはI1、送信元アドレスはI2'となる。パケット1017は、パケット1015と同一である。

【0176】(G-2-2-1)内部ホストから端末への送信

まず、内部ホスト1001から端末1003へパケットを送信する場合の動作を説明する。

【0177】内部ホスト1001は、トンネリング処理部1006にパケット1012を入力する。トンネリング処理部1006は、パケット1012を暗号処理しカプセル化しパケット1013を得る。この時、パケット1012の受信先アドレスがI2であるので、パケット1013の受信先アドレスをI2'にする。トンネリング処理部1006は、「通信路C」1002にパケット1013を送信する。トンネリング処理部1010は、「通信路C」1002からパケット1013を受信する。

【0178】トンネリング処理部1010は、パケット1013を脱カプセル化し復号処理しパケット1014を得る。

【0179】(G-2-2-2)端末から内部ホストへの送信

逆に、端末1003から内部ホスト1001へパケットを送信する場合の動作を説明する。

【0180】端末1003は、トンネリング処理部1010にパケット1015を入力する。トンネリング処理部1010は、パケット1015を暗号処理しカプセル化しパケット1016を得る。この時、パケット1015の受信先アドレスがI1であるので、パケット1016の受信先アドレスをI1とする。トンネリング処理部1010は、「通信路C」1002にパケット1016を送信する。トンネリング処理部1006は、「通信路C」1002からパケット1016を受信する。トンネリング処理部1006は、パケット1016を脱カプセル化し復号処理しパケット1017を得る。

【0181】内部ホスト1001は、パケット1017を得る。

【0182】(G-3)第6の実施形態の効果

以上のように、第6の実施形態によれば、内部ネットワークの他のサブネットへ移動した端末と内部ホストの間にトンネルを設けるので、端末を内部ネットワークの他のサブネットへ移動しても、端末は移動前のサービス利用権限で内部ホストが提供するサービスを利用できるという効果が得られる。

【0183】勿論、第6の実施形態では、複数の内部ホストと複数の端末が同時に通信可能である。

【0184】(H)第7の実施形態

続いて、第7の実施形態を説明する。ところで、第2、第3、第4、第5、第6の実施形態では、内部ホストと

とに、端末までトンネルを設ける機能を備える必要がある。そこで、次の構成を考える。

【0185】(H-1)第7の実施形態の構成

図11は、第7の実施形態の構成図である。本実施形態に係る通信システムは、内部ホスト1101、「通信路A」1102、サブネット管理サーバ1103、「通信路B」1104、ファイアウォール1105、「通信路C」1106、端末1107からなる。

【0186】本実施形態に係るサブネット管理サーバ1103は、セッション管理部1108、トンネリング処理部1109を構成要素とする。

【0187】本実施形態に係るファイアウォール1105は、セッション管理部1110、アクセス制御部1111を構成要素とする。

【0188】本実施形態に係る端末1107は、セッション管理部1112、移動前情報記憶部1113、トンネリング処理部1114を構成要素とする。

【0189】「通信路A」1102は、内部ホスト1101とサブネット管理サーバ1103の間の通信路である。すなわち、「通信路A」1102は、内部ネットワークの通信路である。「通信路B」1104は、サブネット管理サーバ1103とファイアウォール1105の間の通信路である。すなわち、「通信路B」1104は、内部ネットワークの通信路である。「通信路C」1106は、ファイアウォール1105と端末1107の間の通信路である。すなわち、「通信路C」1106は、外部ネットワークの通信路である。

【0190】サブネット管理サーバ1103とファイアウォール1105の間にはトンネル1115を設ける。ファイアウォール1105と端末1107の間にはトンネル1116を設ける。

【0191】サブネット管理サーバ1103は、サブネットごとに設ける。サブネット管理サーバ1103が位置するサブネットは、サブネットAである。なお、端末1107は、外部ネットワークへ移動する前にはサブネットAに位置していたものとする。

【0192】端末1107が外部ネットワークへ移動した後で内部ホスト1101と通信する場合に、サブネット管理サーバ1103と端末1107の間のトンネルを抜ける。

【0193】サブネット管理サーバ1103は、内部ホスト1101から端末1107宛てのパケットを受信し、そのパケットを暗号処理しカプセル化して、トンネルを通して端末1107へ送信する。また、サブネット管理サーバ1103は、トンネルを通して端末1107から内部ホスト1101宛てのパケットを受信し、そのパケットを脱カプセル化し復号処理して、内部ホスト1101へ送信する。サブネット管理サーバ1103のアドレスは、Sである。

【0194】内部ホスト1101は、端末1107の



ドレスとして移動前アドレス12を使用して、パケットを「通信路A」1102と送受信する。端末1107は、端末1107のアドレスとして移動前アドレス12を使用して、パケットをトンネリング処理部1114と入出力する。

【0195】セッション管理部1110とセッション管理部1112は、互いに通信し、端末1107の認証と鍵交換をする。セッション管理部1112は、セッション管理部1110へ、端末1107が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスが12であること、サブネット管理サーバ1103のアドレスがSであることを通知する。セッション管理部1110は、セッション管理部1108へ、端末1107が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスが12であること、鍵を通知する。

【0196】トンネリング処理部1109は、セッション管理部1110が交換した鍵を使用して、端末1107宛てのパケットを暗号処理してカプセル化する。また、トンネリング処理部1109は、内部ホスト1101宛てのパケットを脱カプセル化し復号処理する。

【0197】トンネリング処理部1114は、セッション管理部1112が交換した鍵を使用して、内部ホスト1101宛てのパケットを暗号処理してカプセル化する。

【0198】また、トンネリング処理部1114は、端末1107宛てのパケットを脱カプセル化し復号処理する。

【0199】移動前情報記憶部1113は、端末1107の移動前アドレス12と、サブネット管理サーバ1103のアドレスSを、記憶する。

【0200】アクセス制御部1111は、受信するパケットが、サブネット管理サーバ1103と端末1107の間の通信のパケットであるかを判定する。アクセス制御部1111は、サブネット管理サーバ1103と端末1107の間の通信のパケットを、中継する。アクセス制御部1111は、サブネット管理サーバ1103と端末1107の間の通信ではないパケットを、中継しない。

【0201】(H-2)第7の実施形態の動作  
続いて、図11に示す通信システムによって実現される通信動作を説明する。

【0202】(H-2-1)通信開始前の動作  
まず、内部ホスト1101と端末1107が通信を開始するまでの動作を説明する。

【0203】セッション管理部1110とセッション管理部1112が通信し、端末1107の認証と鍵交換をする。セッション管理部1112は、セッション管理部1110へ、端末1107が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アド

レスが12であること、サブネット管理サーバ1103のアドレスがSであることを通知する。セッション管理部1110は、セッション管理部1108へ、端末1107が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスが12であること、鍵を通知する。

【0204】(H-2-2)通信開始後の動作

次に、内部ホスト1101と端末1107が、通信をする時の動作を説明する。なお、内部ホスト1101から端末1107へ伝送されるパケット1117の受信先アドレスは12、送信元アドレスは11となる。また、パケット1118は、このパケット1117をカプセル化したパケットであり、その受信先アドレスはE、送信元アドレスはSとなる。パケット1119は、パケット1118と同一である。パケット1120は、パケット1117と同一である。

【0205】一方、端末1107から内部ホスト1101へ伝送されるパケット1121の受信先アドレスは11、送信元アドレスは12となる。パケット1122は、このパケット1121をカプセル化したパケットであり、その受信先アドレスはS、送信元アドレスはEとなる。パケット1123は、パケット1122と同一である。パケット1124は、パケット1121と同一である。

【0206】(H-2-2-1)内部ホストから端末への送信

まず、内部ホスト1101から端末1107にパケットを送信する場合の動作を説明する。

【0207】内部ホスト1101は、「通信路A」1102にパケット1117を送信する。

【0208】サブネット管理サーバ1103のトンネリング処理部1109は、「通信路A」1102からパケット1117を受信する。トンネリング処理部1109は、パケット1117を暗号処理しカプセル化しパケット1118を得る。この時、パケット1117の受信先アドレスが12であるので、パケット1118の受信先アドレスをEにする。トンネリング処理部1109は、パケット1118を「通信路B」1104に送信する。アクセス制御部1111は、「通信路B」1104からパケット1118を受信する。

【0209】ファイアウォール1105のアクセス制御部1111は、パケット1118がサブネット管理サーバ1103と端末1107の間の通信のパケットであると判定する。アクセス制御部1111は、パケット1118を「通信路C」1106へ送信する。

【0210】端末1107がパケット1120を得るまでの動作は、実施形態2の動作と同様である。

【0211】(H-2-2-2)端末から内部ホストへの送信

逆に、端末1107から内部ホスト1101にパケット

10

20

30

40

50

を送信する場合の動作を説明する。

【0212】端末1107は、パケット1121をトンネリング処理部1114へ入力する。トンネリング処理部1114は、パケット1121を暗号処理しカプセル化しパケット1122を得る。この時、サブネット管理サーバ1103のアドレスがSであるので、パケット1122の受信先アドレスをSにする。トンネリング処理部1114は、パケット1122を「通信路C」1106へ送信する。アクセス制御部1111は、「通信路C」1106からパケット1122を受信する。ファイ

アウォール1105のアクセス制御部1111は、パケット1122がサブネット管理サーバ1103と端末1107の間の通信のパケットであると判定する。アクセス制御部1111は、パケット1122を「通信路B」1104へ送信する。

【0213】サブネット管理サーバ1103のトンネリング処理部1109は、「通信路B」1104からパケット1123を受信する。トンネリング処理部1109は、パケット1123を脱カプセル化し復号処理し、パ

ケット1124を得る。トンネリング処理部1109は、「通信路A」1102へパケット1124を送信する。

【0214】内部ホスト1101は、パケット1124を受信する。

【0215】(H-3)第7の実施形態の効果  
以上のように、第7の実施形態によれば、端末との間にトンネルを設けるコンピュータ(サブネット管理サーバ)をサブネットごとに設けるので、内部ホストごとに、端末までトンネルを設ける機能を備える必要がなくなるという効果が得られる。

【0216】また、第7の実施形態では、あるサブネット管理サーバ1103と複数の端末1107が同時に通信可能である。また、複数の内部ホスト1101と複数の端末1107が同時に通信可能である。

【0217】さらに、移動前情報記憶部1113がサブネット管理サーバ1103のアドレスSを記憶することと、セッション管理部1112がセッション管理部1110にサブネット管理サーバ1103のアドレスがSであることを通知することの代わりに、セッション管理部1110が、端末1107の移動前アドレスからサブ

ネット管理サーバ1103のアドレスを求める方式も実施可能である。

【0218】(I)第8の実施形態

続いて、第8の実施形態を説明する。ところで、第7の実施形態では、外部ネットワークで、ヘッダにサブネット管理サーバのアドレスを含むパケットを伝送しているため、外部ネットワークに、サブネット管理サーバのアドレスを隠蔽できない。そこで、次の構成を考える。

【0219】(I-1)第8の実施形態の構成

図12は、第8の実施形態の構成図である。図12は、

図11との対応部分に対応符号を付して示したものである。従って、内部ホスト1201～トンネル1216までの構成は、図11の内部ホスト1101～トンネル1116までと同様である。また、パケットのうち、1217、1220、1221、1224は、それぞれ、図11のパケット、1117、1120、1121、1124と同様である。

【0220】相違点は、ファイアウォール1205にアドレス変換部1225が設けられている点である。このアドレス変換部1225は、ファイアウォール1205のアクセス制御部1211が中継するパケットのヘッダのアドレスを書き換える。

【0221】(I-2)第8の実施形態の動作  
ここでは、第8の実施形態の動作のうち、第7の実施形態の動作とは異なる動作を説明する。

【0222】(I-2-1)通信開始前の動作  
まず、内部ホスト1201と端末1207が通信を開始するまでの動作を説明する。

【0223】この場合も、各セッション管理部1208、1210、1212が通信し、認証と鍵交換、また、移動情報やアドレスを確認し合う。

【0224】パケット1218は、内部ホスト1201から端末1207へ送信されるパケット1217をカプセル化したパケットであり、その受信先アドレスはFi、送信元アドレスはSとなる。パケット1219は、このパケット1218のヘッダのアドレスを書き換えたパケットであり、その受信先アドレスはE、送信元アドレスはFeとなる。

【0225】一方、パケット1222は、端末1207から内部ホスト1201へ送信されるパケット1221をカプセル化したパケットであり、その受信先アドレスはFe、送信元アドレスはEとなる。パケット1223は、このパケット1222のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはS、送信元アドレスはFiとなる。

【0226】(I-2-2)通信開始後の動作

(I-2-2-1)内部ホストから端末への送信

まず、内部ホスト1201から端末1207にパケットを送信する場合の動作を説明する。

【0227】アクセス制御部1211は、パケット1218をアドレス変換部1225に入力する。アドレス変換部1225は、パケット1218のヘッダのアドレスを書き換えパケット1219を得る。この時、パケット1218の送信元アドレスがSであるので、パケット1219の受信先アドレスをEにする。

【0228】アドレス変換部1225は、パケット1219をアクセス制御部1211へ出力する。

【0229】(I-2-2-2)端末から内部ホストへの送信

逆に、端末1207から内部ホスト1201にパケット

を送信する場合の動作を説明する。

【0230】アクセス制御部1211は、パケット1222をアドレス変換部1225に入力する。アドレス変換部1225は、パケット1222のヘッダのアドレスを書き換え、パケット1223を得る。この時、パケット1222の送信元アドレスがEであるので、パケット1223の受信先アドレスをSにする。

【0231】アドレス変換部1225は、パケット1223をアクセス制御部1211に出力する。

【0232】(I-3)第8の実施形態の効果  
 10 以上のように、第8の実施形態によれば、ファイアウォールにアドレスを変換する機能を備えたので、外部ネットワークに、サブネット管理サーバのアドレスを隠蔽できるという効果が得られる。

【0233】(J)第9の実施形態

続いて、第9の実施形態を説明する。ところで、第8の実施形態では、あるサブネット管理サーバ1203とは同時に一つの端末しか通信できない。そこで、次の構成を考える。

【0234】(J-1)第9の実施形態の構成

図13は、第9の実施形態の構成図である。図13は、図12との対応部分に対応符号を付したものであり、基本構成は同様である。異なるのは、ファイアウォール1305の有するアドレスである。

【0235】本実施形態におけるファイアウォール1305が、外部ネットワークに接続しているネットワーク・インターフェースのアドレスは一つ、すなわち、アドレスFeである。一方、ファイアウォール1305が、内部ネットワークに接続しているネットワーク・インターフェースのアドレスは、複数のアドレスFi1~Fi  
 30 m(m>1)である。

【0236】セッション管理部1310とセッション管理部1312は、互いに通信し、端末1307の認証と鍵交換をする。

【0237】セッション管理部1312は、セッション管理部1310へ、端末1307が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、サブネット管理サーバ1303のアドレスがSであることを通知する。

【0238】セッション管理部1310は、Fi1~Fi  
 40 mのうち、その時点で使用していないアドレスFijを求める。セッション管理部1310は、セッション管理部1308へ、端末1307が外部ネットワークへ移動したこと、移動前アドレスがI2であること、内部ホスト1301と端末1307の通信で使用するファイアウォール1305の内部アドレスがFijであること、鍵を通知する。

【0239】(J-2)第9の実施形態の動作  
 次に、第9の実施形態の動作を説明する。

【0240】(J-2-1)通信開始前の動作

まず、内部ホスト1301と端末1307が通信を開始するまでの動作を説明する。

【0241】セッション管理部1310とセッション管理部1312は、互いに通信し、端末1307の認証と鍵交換をする。

【0242】端末1307のセッション管理部1312は、セッション管理部1310へ、端末1307が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、サブネット管理サーバ1303のアドレスがSであることを通知する。

【0243】ファイアウォール1305のセッション管理部1310は、Fi1~Fimのうち、その時点で使用していないアドレスFijを求める。セッション管理部1310は、セッション管理部1308へ、端末1307が外部ネットワークへ移動したこと、移動前アドレスがI2であること、内部ホスト1301と端末1307の通信で使用するファイアウォール1305の内部アドレスがFijであること、鍵を通知する。

20 【0244】(J-2-2)通信開始後の動作

内部ホスト1301と端末1307が通信する場合の動作を説明する。第9の実施形態の動作のうち、第8の実施形態の動作とは異なる動作を説明する。

【0245】パケット1318は、内部ホスト1301から端末1307へ伝送されるパケット1317をカプセル化したパケットであり、その受信先アドレスはFij、送信元アドレスはSとなる。パケット1319は、このパケット1318のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはE、送信元アドレスはFeとなる。

30 【0246】パケット1322は、端末1307から内部ホスト1301へ伝送されるパケット1321をカプセル化したパケットであり、その受信先アドレスはFe、送信元アドレスはEとなる。パケット1323は、このパケット1322のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはS、送信元アドレスはFijとなる。

【0247】(J-2-2-1)内部ホストから端末への送信

40 まず、内部ホスト1301から端末1307にパケットを送信する場合の動作を説明する。

【0248】トンネリング処理部1309は、パケット1317を暗号処理しカプセル化しパケット1318を得る。この時、パケット1317の受信先アドレスがI2であるので、パケット1318の受信先アドレスをFijにする。

50 【0249】アドレス変換部1325は、パケット1318のヘッダのアドレスを書き換えパケット1319を得る。この時、パケット1318の受信先アドレスがFijであるので、パケット1319の受信先アドレスを

Eにする。

【0250】(J-2-2-2) 端末から内部ホストへの送信

逆に、端末1307から内部ホスト1301にパケットを送信する場合の動作を説明する。

【0251】アドレス変換部1325は、パケット1322のヘッダのアドレスを書き換え、パケット1323を得る。この時、パケット1322の送信元アドレスがEであるので、パケット1323の受信先アドレスをSにする。

【0252】(J-3) 第9の実施形態の効果  
以上のように、第9の実施形態によれば、ファイアウォール1305に、複数の内部アドレスを割り当てるようにしたので、あるサブネット管理サーバ1303と同時に複数の端末1307が通信できるという効果が得られる。

【0253】(K) 第10の実施形態  
続いて、第10の実施形態を説明する。ところで、第9の実施形態では、ファイアウォールに、複数の内部アドレスを割り当てる必要がある。そこで、第10の実施形態においては、パケットがサブネット管理サーバとどの端末の間の通信のパケットであるかをSPIにより表すことにする。

【0254】(K-1) 第10の実施形態の構成  
図14は、第10の実施形態の構成図である。図14は、第8の実施形態の説明に用いた図12との対応部分に対応符号を付して示したものであり、基本的な構成は同じである。

【0255】セッション管理部1410とセッション管理部1412は、互いに通信し、端末1407の認証と鍵交換をする。

【0256】端末1407のセッション管理部1412は、サブネット管理サーバ1403が端末1407へ送信するパケットのSPI(ここではBとする。)を求める。セッション管理部1412は、セッション管理部1410へ、端末1407が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、サブネット管理サーバ1403のアドレスがSであること、サブネット管理サーバ1403が端末1407へ送信するパケットのSPIがBであることを、通知する。

【0257】ファイアウォール1405のセッション管理部1410は、セッション管理部1408へ、端末1407が外部ネットワークへ移動したこと、移動前アドレスがI2であること、サブネット管理サーバ1403が端末1407へ送信するパケットのSPIがBであること、鍵を通知する。

【0258】セッション管理部1408は、端末1407が内部ホスト1401へ送信するパケットSPI(ここでは、Aとする。)を求める。セッション管理部14

08は、セッション管理部1410へ、端末1407が内部ホスト1401へ送信するパケットのSPIがAであることを通知する。セッション管理部1410はセッション管理部1412へ、端末1407が内部ホスト1401へ送信するパケットのSPIがAであることを通知する。

【0259】サブネット管理サーバ1403のトンネリング処理部1409は、パケット1417をカプセル化する時に、SPIをBにする。

10 【0260】端末1407のトンネリング処理部1414は、パケット1421をカプセル化するとき、SPIをAにする。

【0261】ファイアウォール1405のアドレス変換部1425は、SPIにより、パケットのヘッダのアドレスを書き換える。

【0262】(K-2) 第10の実施形態の動作  
次に、第10の実施形態の動作を説明する。なお、第10の実施形態の動作のうち、第8の実施形態の動作とは異なる動作のみを説明する。

20 【0263】(K-2-1) 通信開始後の動作  
内部ホスト1401と端末1407が通信する場合の動作を説明する。

【0264】パケット1418は、内部ホスト1401から端末1407へ伝送されるパケット1417をカプセル化したパケットであり、その受信先アドレスはFi、送信元アドレスはS、SPIはBとなる。パケット1419は、このパケット1418のヘッダアドレスを書き換えたパケットであり、その受信先アドレスはE、送信元アドレスはFe、SPIはBとなる。

30 【0265】パケット1422は、端末1407から内部ホスト1401へ伝送されるパケット1421をカプセル化したパケットであり、その受信先アドレスはFe、送信元アドレスはE、SPIはAとなる。パケット1423は、パケット1422のヘッダのアドレスを書き換えたパケットであり、受信先アドレスはS、送信元アドレスはFi、SPIはAとなる。

【0266】(K-2-1-1) 内部ホストから端末への送信

40 まず、内部ホスト1401から端末1407にパケットを送信する場合の動作を説明する。

【0267】トンネリング処理部1409は、パケット1417を暗号処理しカプセル化しパケット1418を得る。この時、パケット1417の受信先アドレスがI2であるので、SPIをBにする。アドレス変換部1425は、パケット1418のヘッダのアドレスを書き換え、パケット1419を得る。この時、パケット1418のSPIがBであるので、パケット1419の受信先アドレスをEとする。

【0268】(K-2-1-2) 端末から内部ホストへの送信

逆に、端末 1407 から内部ホスト 1401 にパケットを送信する場合の動作を説明する。

【0269】アドレス変換部 1425 は、パケット 1422 のヘッダのアドレスを書き換え、パケット 1423 を得る。この時、パケット 1422 の送信元アドレスが E であるので、パケット 1423 の受信先アドレスを S とする。

【0270】(K-3) 第 10 の実施形態の効果  
 以上のように、第 10 の実施形態によれば、パケットのヘッダに書き込まれている SPI により、パケットがどのサブネット管理サーバとどの端末の間の通信のパケットであるかを表すようにしたので、ファイアウォールに複数の内部アドレスを割り当てなくても、あるサブネット管理サーバと複数の端末が同時に通信できるようになるという効果が得られる。

【0271】(L) 第 11 の実施形態  
 続いて、第 11 の実施形態を説明する。ところで、第 7、第 8、第 9、第 10 の実施形態では、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネットへ移動すると、端末のアドレスが変化するので、端末は移動前のサービス利用権限で内部ホストが提供するサービスを利用できなくなる。そこで、次の構成を考える。なお、第 11 の実施形態では、端末が外部ネットワークに移動する場合に係る構成及び動作は、第 7 の実施形態の場合と同様である。

【0272】(L-1) 第 11 の実施形態の構成  
 図 15 は、第 11 の実施形態の構成図である。図 15 には、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネットへ移動する場合に係る構成要素を示している。また、図 15 には、端末を外部ネットワークへ移動する場合に係る構成要素の一部を示す。従って、図 15 に示されている、内部ホスト 1501、「通信路 A」1502、サブネット管理サーバ 1503、「通信路 D」1504、端末 1505 の他に、不図示のファイアウォールがある。

【0273】本実施形態に係るサブネット管理サーバ 1503 は、外部セッション管理部 1506、内部セッション管理部 1507、トンネリング処理部 1508 を構成要素としてもつ。

【0274】本実施形態に係る端末 1505 は、内部セッション管理部 1509、外部セッション管理部 1510、移動前情報記憶部 1511、トンネリング処理部 1512 を構成要素としてもつ。

【0275】サブネット管理サーバ 1503 は、サブネット A に位置する。

【0276】端末 1505 は、内部ネットワークでの移動前にサブネット A に位置し、内部ネットワークでの移動後にサブネット B に位置する。

【0277】「通信路 A」1502 は、内部ホスト 1501 とサブネット管理サーバ 1503 の間の通信路であ

る。すなわち、「通信路 A」1502 は、内部ネットワークの通信路である。「通信路 D」1504 は、サブネット管理サーバ 1503 と端末 1505 の間の通信路である。すなわち、「通信路 D」1504 は、内部ネットワークの通信路である。

【0278】サブネット管理サーバ 1503 と端末 1505 の間にはトンネル 1513 を設ける。

【0279】内部セッション管理部 1507 と内部セッション管理部 1509 は、互いに通信し、端末 1505 の認証と鍵交換をする。

【0280】内部セッション管理部 1509 は、内部セッション管理部 1507 へ、端末 1505 が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスが I2' であること、移動前アドレスが I2 であることを通知する。

【0281】トンネリング処理部 1508 は、内部セッション管理部 1507 が交換した鍵を使用して、端末 1505 宛てのパケットを暗号処理してカプセル化する。

【0282】また、トンネリング処理部 1508 は、外部セッション管理部 1506 が交換した鍵を使用して、外部ネットワークに移動した端末宛てのパケットを暗号処理してカプセル化する。トンネリング処理部 1508 は、内部ホスト 1501 宛てのパケットを脱カプセル化し復号処理する。

【0283】トンネリング処理部 1512 は、内部セッション管理部 1509 が交換した鍵を使用して、内部ホスト 1501 宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部 1512 は、外部セッション管理部 1510 が交換した鍵を使用して、内部ホスト 1501 宛てのパケットを暗号処理しカプセル化する。トンネリング処理部 1512 は、端末 1505 宛てのパケットを脱カプセル化し復号処理する。

【0284】移動前情報記憶部 1511 は、端末 1505 の移動前アドレス I2 とサブネット管理サーバ 1503 のアドレス S を記憶する。

【0285】第 7 の実施形態と同様に、ファイアウォールの構成要素は、セッション管理部とアクセス制御部である。サブネット管理サーバ 1503 とファイアウォールの間には、「通信路 B」とトンネルがある。ファイアウォールと外部ネットワークに移動した端末の間には、「通信路 C」とトンネルがある。

【0286】外部セッション管理部 1510 とファイアウォールのセッション管理部は、互いに通信し、外部ネットワークに移動した端末の認証と鍵交換をする。外部セッション管理部 1510 は、ファイアウォールのセッション管理部へ、端末が外部ネットワークへ移動したこと、移動後のアドレスが E であること、移動前アドレスが I2 であることを、サブネット管理サーバ 1503 のアドレスが S であることを通知する。

【0287】ファイアウォールのセッション管理部は、

外部セッション管理部1506へ、端末が外部ネットワークへ移動したこと、移動後のアドレスがEであること、移動前アドレスがI2であること、鍵を通知する。

【0288】(L-2)第11の実施形態の動作次に、第11の実施形態の動作を説明する。なお、第11の実施形態の動作のうち、第7の実施形態の動作とは異なる動作のみを説明する。

【0289】(L-2-1)通信開始前の動作内部ホスト1501と端末1505の通信の開始における動作を説明する。

【0290】内部セッション管理部1507と内部セッション管理部1509は、互いに通信し、端末1505の認証と鍵交換をする。

【0291】端末1505の内部セッション管理部1509は、セッション管理部1507へ、端末1505が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがI2'であること、移動前アドレスがI2であることを通知する。

【0292】(L-2-2)通信開始後の動作次に、内部ホスト1501と端末1505が通信をする時の動作を説明する。

【0293】内部ホスト1501から端末1505へ伝送されるパケット1514の受信先アドレスはI2、送信元アドレスはI1となる。このパケット1514をカプセル化したパケット1515の受信先アドレスはI2'、送信元アドレスはSとなる。パケット1516は、パケット1514と同一である。

【0294】端末1505から内部ホスト1501へ伝送されるパケット1517の受信先アドレスはI1、送信元アドレスはI2となる。このパケット1517をカプセル化したパケット1518の受信先アドレスはS、送信元アドレスはI2'となる。パケット1519は、パケット1517と同一である。

【0295】(L-2-2-1)内部ホストから端末への送信

まず、内部ホスト1501から端末1505へパケットを送信する場合の動作を説明する。

【0296】サブネット管理サーバ1503のトンネリング処理部1508は、パケット1514を暗号処理しカプセル化しパケット1515を得る。この時、パケット1514の受信先アドレスがI2であるので、パケット1515の受信先アドレスをI2'にする。

【0297】(L-2-2-2)端末から内部ホストへの送信

逆に、端末1505から内部ホスト1501へパケットを送信する場合の動作を説明する。

【0298】端末1505のトンネリング処理部1512は、パケット1517を暗号処理しカプセル化しパケット1518を得る。この時、サブネット管理サーバ1503のアドレスがSであるので、パケット1518の

受信先アドレスをSにする。

【0299】外部ネットワークに移動した端末と内部ホストの通信に関しては、第7の実施形態の動作と同様である。

【0300】(L-3)第11の実施形態の効果以上のように、第11の実施形態によれば、サブネット管理サーバと、内部ネットワークの他のサブネットへ移動した端末の間にトンネルを設けるので、端末が内部ネットワークの他のサブネットに移動しても、内部ホストが提供するサービスを移動前のサービス利用権限で利用できるという効果が得られる。

【0301】また、第11の実施形態では、あるサブネット管理サーバ1503と複数の端末1505が同時に通信可能である。

【0302】(M)第12の実施形態続いて、第12の実施形態を説明する。ところで、第11の実施形態では、端末1505がトンネリングの処理をする必要がある。そこで、次の構成を考える。なお、第12の実施形態では、端末が外部ネットワークに移動する場合に係る構成、動作は、第7の実施形態と同じである。

【0303】(M-1)第12の実施形態の構成図16は、第12の実施形態の構成図である。図16には、内部ネットワークのあるサブネットに位置する端末を、内部ネットワークの他のサブネットへ移動する場合に係る構成要素を示す。また、図16には、端末を外部ネットワークへ移動する場合に係る構成要素の一部を示す。従って、図16に示されている、内部ホスト1601、「通信路A」1602、「サブネット管理サーバA」1603、「通信路E」1604、「サブネット管理サーバB」1605、「通信路F」1606、端末1607、他に、不図示のファイアウォールがある。

【0304】ここで、「サブネット管理サーバA」1603は、サブネットAに位置する。「サブネット管理サーバB」1605は、サブネットBに位置する。端末1607が移動前に位置するサブネットは、サブネットAである。端末1607が移動後に位置するサブネットは、サブネットBである。

【0305】「サブネット管理サーバA」1603は、外部セッション管理部1608、内部セッション管理部1609、トンネリング処理部1610を構成要素とする。一方、「サブネット管理サーバB」1605は、内部セッション管理部1611、外部セッション管理部1612、トンネリング処理部1613を構成要素とする。

【0306】端末1607は、内部セッション管理部1614、外部セッション管理部1615、移動前情報記憶部1616、トンネリング処理部1617を構成要素とする。

【0307】内部ホスト1601と「サブネット管理サ

サーバA」1603の間には「通信路A」1602を設ける。この「通信路A」1602は、内部ネットワークの通信路である。「サブネット管理サーバA」1603と「サブネット管理サーバB」1605の間には「通信路E」1604を設ける。この「通信路E」1604は、内部ネットワークの通信路である。「サブネット管理サーバB」1605と端末1607の間には「通信路F」1606を設ける。この「通信路F」1606は、内部ネットワークの通信路である。

【0308】「サブネット管理サーバA」1603と「サブネット管理サーバB」1605の間にはトンネル1618を設ける。

【0309】内部セッション管理部1609と内部セッション管理部1614は、互いに通信し、端末1607の認証と鍵交換をする。

【0310】内部セッション管理部1614は、内部セッション管理部1609へ、端末1607が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがI2'であること、移動前アドレスがI2であることを通知する。

【0311】内部セッション管理部1609は、端末1607の移動後のアドレスI2'から、「サブネット管理サーバB」のアドレスS2を求める。内部セッション管理部1609は、内部セッション管理部1611へ、端末1607がサブネットBへ移動したこと、端末1607の移動前アドレスがI2であること、「サブネット管理サーバA」のアドレスがS1であること、鍵を通知する。

【0312】トンネリング処理部1610は、内部セッション管理部1609が交換した鍵を使用して、端末1607宛てのパケットを暗号処理してカプセル化する。

【0313】また、トンネリング処理部1610は、ファイアウォールのセッション管理部が外部セッション管理部1608に通知した鍵を使用して、外部ネットワークへ移動した端末宛てのパケットを暗号処理してカプセル化する。トンネリング処理部1610は、内部ホスト1601宛てのパケットを脱カプセル化し復号処理する。

【0314】トンネリング処理部1613は、内部セッション管理部1609が内部セッション管理部1611に通知した鍵を使用して、内部ホスト1601宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部1613は、ファイアウォールのセッション管理部が外部セッション管理部1612に通知した鍵を使用して、外部ネットワークへ移動した端末宛てのパケットを暗号処理しカプセル化する。トンネリング処理部1613は、端末1607宛てのパケットを脱カプセル化し復号処理する。

【0315】トンネリング処理部1617は、外部セッション管理部1615が交換した鍵を使用して、内部ホ

スト1601宛てのパケットを暗号処理しカプセル化する。また、トンネリング処理部1617は、外部ネットワークに移動した端末宛てのパケットを脱カプセル化し復号処理する。

【0316】移動前情報記憶部1616は、端末1607の移動前アドレスI2と「サブネット管理サーバA」1603のアドレスS1を記憶する。

【0317】第7の実施形態と同様に、ファイアウォールの構成要素は、セッション管理部とアクセス制御部である。「サブネット管理サーバA」1603とファイアウォールの間には、「通信路B」とトンネルがある。

「サブネット管理サーバB」1605とファイアウォールの間には別の通信路と別のトンネルがある。ファイアウォールと外部ネットワークに移動した端末の間には、「通信路C」とトンネルがある。

【0318】(M-2)第12の実施形態の動作次に、第12の実施形態の動作を説明する。なお、第12の実施形態の動作のうち、第7の実施形態の動作とは異なる動作のみを説明する。

【0319】(M-2-1)通信開始前の動作

まず、内部ホスト1601と端末1607の通信の開始における動作を説明する。

【0320】「サブネット管理サーバA」1603の内部セッション管理部1609と端末1607の内部セッション管理部1614は、互いに通信し、端末1607の認証と鍵交換をする。

【0321】端末1607の内部セッション管理部1614は、内部セッション管理部1609へ、端末1607が内部ネットワークの他のサブネットに移動したこと、移動後のアドレスがI2'であること、移動前アドレスがI2であることを通知する。

【0322】「サブネット管理サーバA」1603の内部セッション管理部1609は、端末1607の移動後のアドレスI2'から、「サブネット管理サーバB」のアドレスS2を求める。内部セッション管理部1609は、内部セッション管理部1611へ、端末1607がサブネットBへ移動したこと、端末1607の移動前アドレスがI2であること、サブネット管理サーバA1603のアドレスがS1であること、鍵を通知する。ここで、内部セッション管理部1609と内部セッション管理部1614が通信する時に使用する通信路は、「通信路E」1604と「通信路F」1606であっても、図16に示さない別の通信路であってもよい。

【0323】(M-2-2)通信開始後の動作

次に、内部ホスト1601と端末1607が通信をする時の動作を説明する。

【0324】内部ホスト1601から端末1607へ伝送されるパケット1619の受信先アドレスはI2、送信元アドレスはI1となる。このパケット1619をカプセル化したパケット1620の受信先アドレスはS



2、送信元アドレスはS1となる。パケット1621は、パケット1619と同一である。

【0325】端末1607から内部ホスト1601へ伝送されるパケット1622の受信先アドレスはI1、送信元アドレスはI2となる。このパケット1622をカプセル化したパケット1623の受信先アドレスはS1、送信元アドレスはS2となる。パケット1624は、パケット1622と同一である。

【0326】(M-2-2-1) 内部ホストから端末への送信

まず、内部ホスト1601から端末1607へパケットを送信する場合の動作を説明する。トンネリング処理部1610は、パケット1619を暗号処理しカプセル化し、パケット1620を得る。この時、パケット1619の受信先アドレスがI2であるので、パケット1620の受信先アドレスをS2にする。

【0327】(M-2-2-2) 端末から内部ホストへの送信

逆に、端末1607から内部ホスト1601へパケットを送信する場合の動作を説明する。

【0328】トンネリング処理部1613は、パケット1622を暗号処理しカプセル化しパケット1623を得る。この時、トンネリング処理部1613は、パケット1622の送信元アドレスがI2であるので、パケット1623の受信先アドレスをS1にする。

【0329】(M-3) 第12の実施形態の効果

以上のように、第12の実施形態によれば、サブネット管理サーバの間にトンネルを設けるので、端末がトンネリングの処理をしないので、端末の負荷を軽減できるという効果が得られる。

【0330】また、第12の実施形態では、複数のサブネット管理サーバどうしが同時に通信可能であり、また、複数の内部ホスト1601と複数の端末1607とも同時に通信可能である。

【0331】(N) 他の実施形態

(N-1) なお、上述の各実施形態においては、内部ネットワークに位置する端末を外部ネットワークに移動した場合におけるサービスの利用権限について説明したが、内部ネットワークに一度も位置しないが、内部ネットワーク上のアドレスが割り当てられており、かつ、そのアドレスを記憶している端末についても本システムを適用することができる。すなわち、かかる端末についても、内部ホストのサービスを内部ネットワークでのアドレスに基づくサービス利用権限で利用することができる。

【0332】(N-2) また、上述の各実施形態においては、端末が内部ホストのサービスを利用することを前提として説明したが、内部ネットワークのいずれかのコンピュータが、端末の外部ネットワークでのアドレスを記憶するならば、内部ホストが端末のサービスを利用することもできる。

【0333】(N-3) また、上述の各実施形態においては、パケットを暗号処理する場合についてのみ述べたが、パケットの暗号処理とパケットの認証処理をすることもできる。また、パケットを暗号処理せず、パケットの認証処理だけを行うこともできる。パケットを認証する方式には、従来技術の上記文献に示されるAH (Authentication Header) がある。

【0334】(N-4) また、上述の各実施形態においては、パケットを暗号処理する場合について述べたが、トンネリング処理部で複数の暗号処理のアルゴリズムを使えるようにすると、パケットのヘッダのアドレスにより、暗号処理のアルゴリズムを変える通信方式、パケットのヘッダのSPIにより、暗号処理のアルゴリズムを変える通信方式も実施可能である。ここで、暗号処理のアルゴリズムには、恒等写像を含むものとする。通信路がセキュリティの面で安全であるとみなせる場合には、暗号処理のアルゴリズムは恒等写像でよい。また、通信する情報が既に暗号化されている場合も、暗号処理のアルゴリズムは恒等写像でよい。

【0335】(N-5) また、第5、第10の実施形態においては、パケットのヘッダのSPI (使用する暗号アルゴリズムや鍵などのセキュリティに関係するパラメータを表す) を利用して、パケットのヘッダのアドレスを書き換える場合について述べたが、パケットのヘッダに、パケットが通過するトンネルの両端のアドレスを表すフィールドを設け、そのフィールドの値を利用するようにしても、パケットのヘッダのアドレスを書き換えることができる。

【0336】(N-6) また、第2～第12の実施形態においては、トンネルの端に位置する内部ホスト又はサブネット管理サーバで暗号処理と復号処理とを行っているが、暗号処理と復号処理を、トンネル内部の端以外の位置のコンピュータで行うこともできる。暗号処理と復号処理を、トンネル内部の端以外の位置のコンピュータで行うと、内部ホスト、サブネット管理サーバの負荷を下げることができる。なお、第2～第12の実施形態においては、トンネル内部の端以外の位置のコンピュータは、ファイアウォールである。

【0337】(N-7) また、第2～第12の実施形態においては、外部ネットワークに移動した端末の認証と鍵交換を、ファイアウォールのセッション管理部が行っているが、外部ネットワークに移動した端末の認証と鍵交換を、内部ホスト又はサブネット管理サーバのセッション管理部が行うこともできる。外部ネットワークに移動した端末の認証と鍵交換を、内部ホスト又はサブネット管理サーバのセッション管理部が行うと、ファイアウォールの負荷を下げることができる。

【0338】(N-8) また、上述の各実施形態においては、ファイアウォール、内部ホスト、サブネット管理サーバのいずれかと端末が鍵交換をする場合を例に説明し



たが、鍵交換をする代わりに、固定の鍵を使用することもできる。

#### 【0339】

【発明の効果】以上のように、第1の発明によれば、外部ネットワークに位置する端末が、ファイアウォールを介して内部ネットワークの内部ホストと通信する形態の通信システムにおいて、端末に、移動前に又は予め内部ネットワークにおいて割り当てられた端末アドレスを記憶するアドレス記憶手段を備えるようにする。これにより、外部ネットワークに位置する端末であっても内部ネットワークで割り当てられた端末アドレスを記憶する端末については、内部ホスト側において、当該端末に提供し得るサービスの利用権限を判別することが可能となる。その結果、特定の端末については、外部ネットワークに位置する場合にも、内部ネットワークに位置する場合と同じ利用権限でのサービスを受けることができる通信システムを実現できる。

【0340】また、第2の発明によれば、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内で内部ホストと通信する形態の通信システムにおいて、(1) 端末に、同じネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備えると共に、(2) 端末及び内部ホストに、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及び内部ホストの間に形成したトンネルを介して入出力するトンネリング処理手段を備えるようにする。これにより、端末が、内部ネットワーク内のあるサブネットから他のサブネットに端末が移動した場合にも、移動前のサブネットで許容されていたのと同じ利用権限でサービスを受けることができるようになる。

【0341】さらに、第3の発明によれば、内部ネットワーク内のあるサブネットに位置する端末が、当該ネットワーク内の内部ホストと通信する形態の通信システムにおいて、(1) 端末に、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備えると共に、(2) 端末及び当該端末が移動前に位置したサブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、端末及びサブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えるようにする。これにより、端末が、内部ホストごとに各端末までのトンネルを設けなくて良くなる。

【0342】さらに、第4の発明によれば、内部ネットワーク内のあるサブネットに位置する端末が、当該ネッ

トワーク内の内部ホストと通信する形態の通信システムにおいて、(1) 端末に、同一ネットワーク内のあるサブネットから他のサブネットへ移動した後も、移動前に割り当てられた端末アドレスを記憶し続けるアドレス記憶手段を備えると共に、(2) 端末の移動の前後に係る各サブネットのサブネット管理サーバは、当該移動があった場合に、アドレス記憶手段が記憶している移動前の端末アドレスと同一のアドレスを有するパケットを、カプセル化後、当該サブネット管理サーバ間に形成したトンネルを介して入出力するトンネリング処理手段を備えるようにする。これにより、端末がトンネリング処理をせずに済み、その分、端末の負荷を軽減することができる。

#### 【図面の簡単な説明】

【図1】第1の実施形態に係る通信システムの構成例を示すブロック図である。

【図2】従来のパケット構成を示す説明図である。

【図3】従来の通信システムの構成を示すブロック図である。

【図4】各実施形態で使用するパケット構成を示す説明図である。

【図5】一部の実施形態で使用するパケット構成を示す説明図である。

【図6】第2の実施形態に係る通信システムの構成例を示すブロック図である。

【図7】第3の実施形態に係る通信システムの構成例を示すブロック図である。

【図8】第4の実施形態に係る通信システムの構成例を示すブロック図である。

【図9】第5の実施形態に係る通信システムの構成例を示すブロック図である。

【図10】第6の実施形態に係る通信システムの構成例を示すブロック図である。

【図11】第7の実施形態に係る通信システムの構成例を示すブロック図である。

【図12】第8の実施形態に係る通信システムの構成例を示すブロック図である。

【図13】第9の実施形態に係る通信システムの構成例を示すブロック図である。

【図14】第10の実施形態に係る通信システムの構成例を示すブロック図である。

【図15】第11の実施形態に係る通信システムの構成例を示すブロック図である。

【図16】第12の実施形態に係る通信システムの構成例を示すブロック図である。

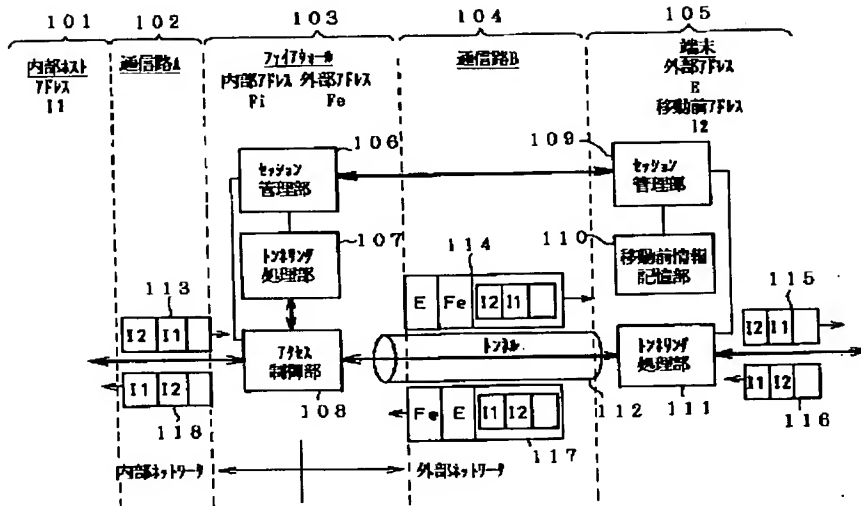
#### 【符号の説明】

501、601…内部ホスト、503、603～903、1105、12051305、1405…ファイアウォール、505、605～905、1003、1107、1207～1407、1505、1607…端末、1103、1203～1603、1605…サブネット

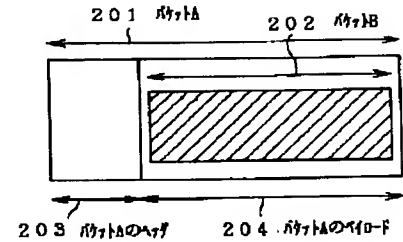
管理サーバ、510、611、711、811、911、1009、1113、1213、1313、1413、1511、1616…移動前情報記憶部、1005、1007、1507、1509、1609、1611

1、1614…内部セッション管理部、1004、1008、1506、1510、1608、1612、1615…外部セッション管理部。

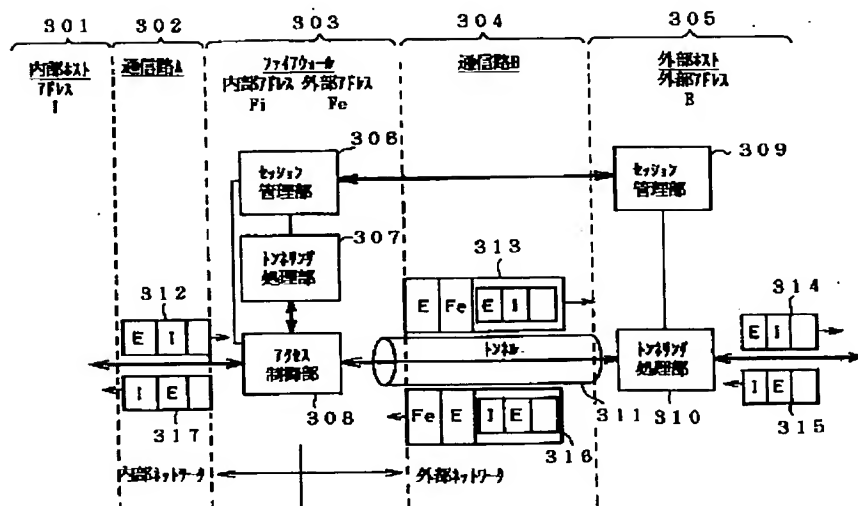
【図1】



【図2】

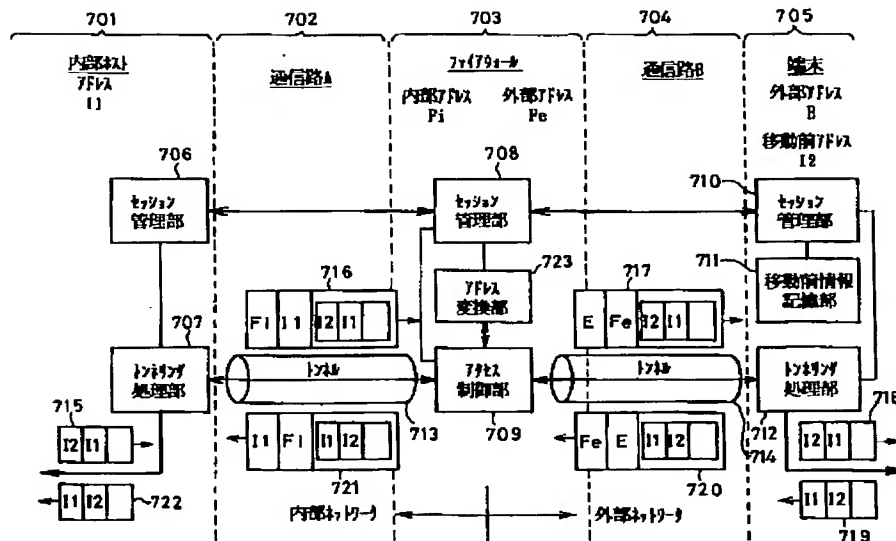


【図3】

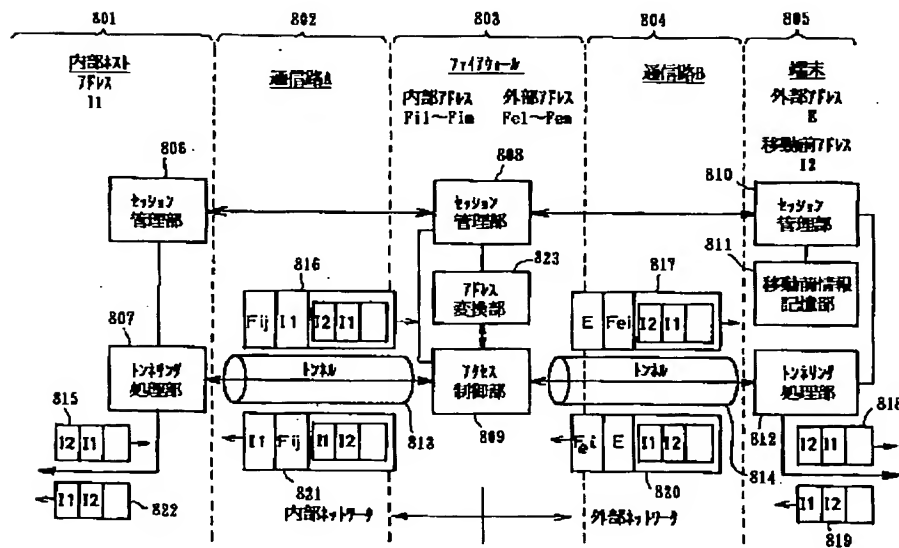




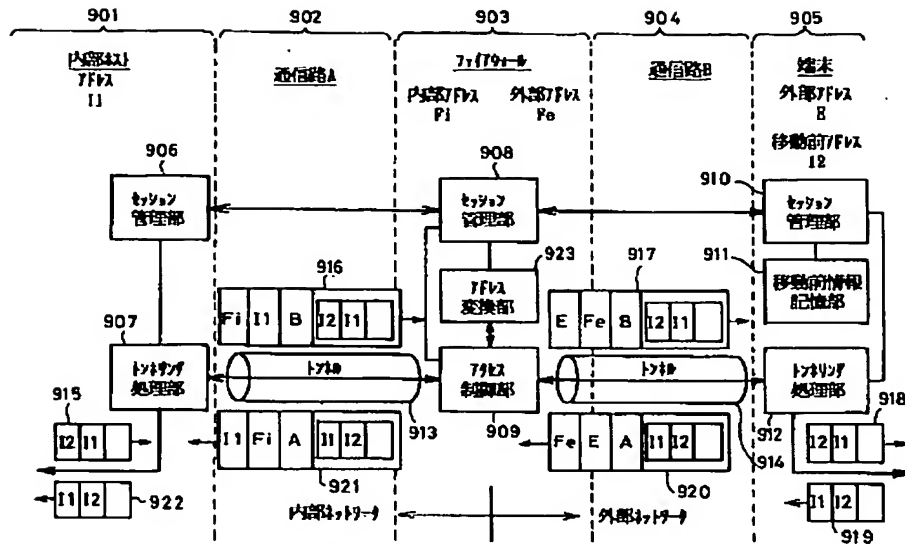
【図 7】



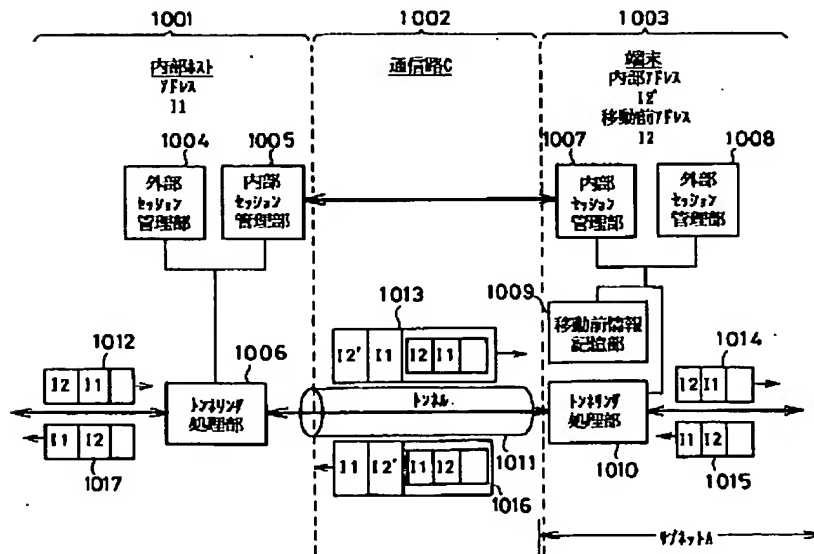
【図 8】



【図 9】

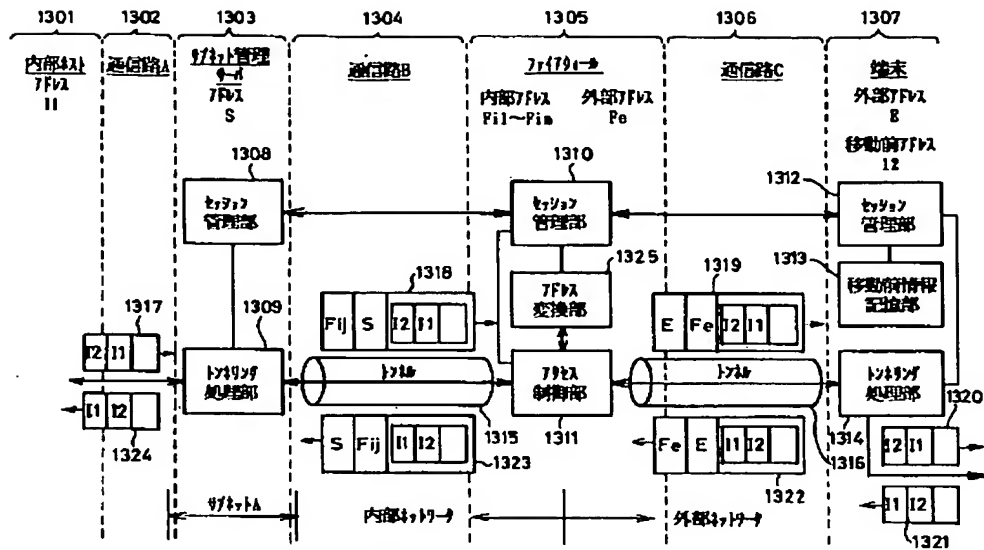


【図 10】

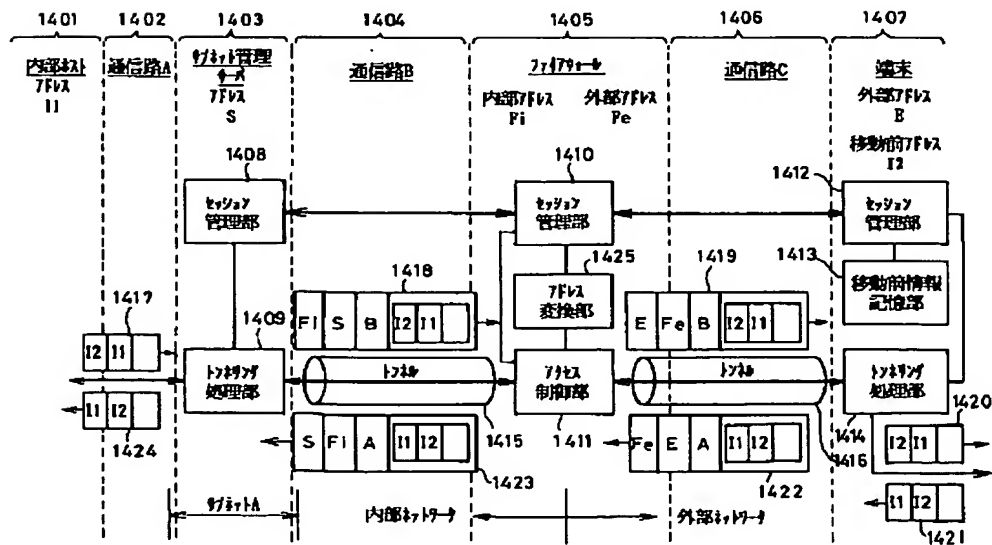




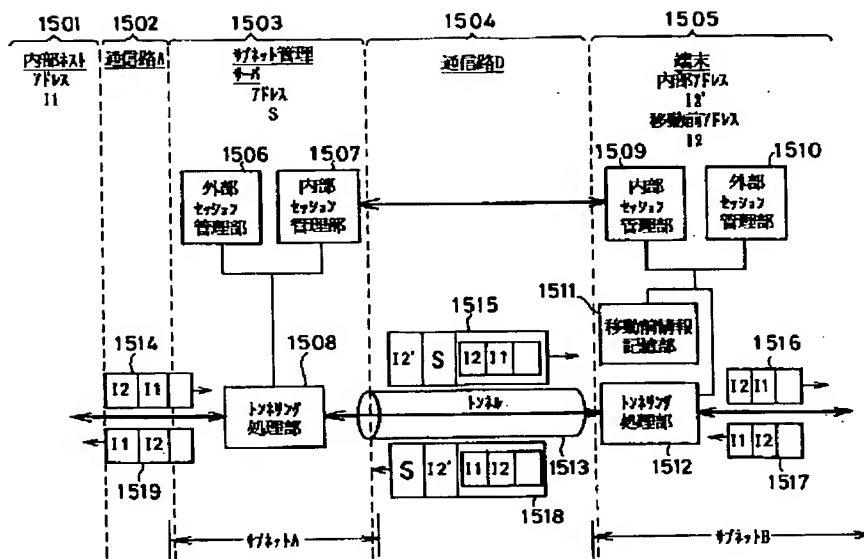
【図 13】



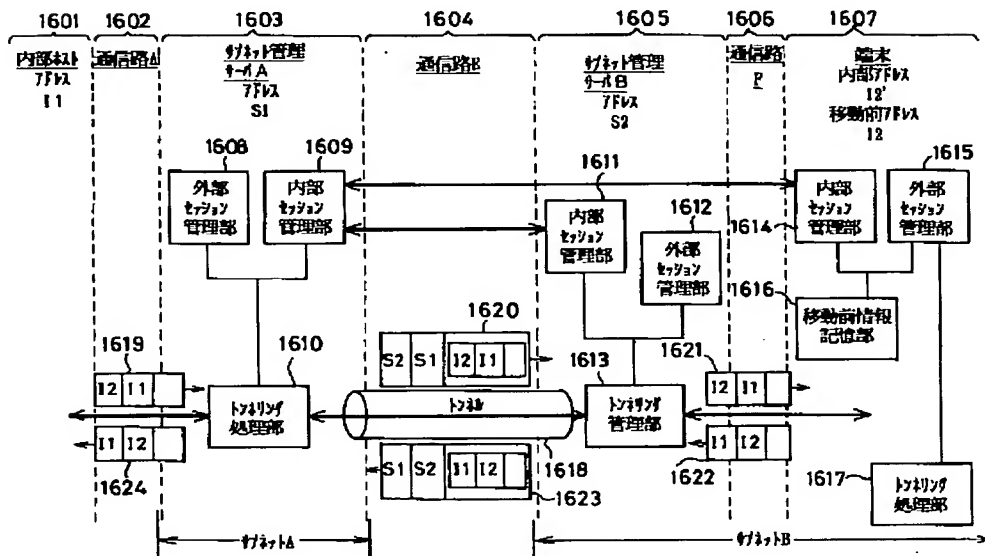
【図 14】



【図15】



【図16】





**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☒ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

THIS PAGE BLANK (1970)